Release Notes for Cisco Unified Communications Manager and IM and Presence Service, Release 10.0(1)

First Published: 2013-12-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-29587-02

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Introduction** 1

About Release Notes 1

Documentation for Release 10.0(1) 2

New and Changed 2

Upgrades 2

CHAPTER 2 **Important Notes** 3

Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets 4

Cisco Unified Mobility Disclaimer 4

Deployment 4

No Configuration During Upgrades 4

Upgrade Considerations for Virtual Machines 5

Upgrades from IM and Presence Service 10.0(1) Export Unrestricted 5

Upgrade Fails if AXL Password Contains Special Characters 5

Directory Search in Self Care 5

DRS Restore of Failed IM and Presence Service Database Publisher Node Requires DRS Restore of Cisco Unified Communications Manager Publisher Node 6

IP Phone SSL VPN not Supported on Third Party Firewalls 6

Increase in Number of LDAP Sync Agreements 6

Jabber Certificate Warnings with IM and Presence Service 6

Parameter Settings 7

Removal of Simplified Messaging Desk Interface (SMDI) and Music-On-Hold Live-Audio Source 7

Self Care Breaks User Call Fwd Settings 7

Self Care Portal Does Not Recognize the Default Voicemail Profile or Pilot 8

TFTP Server Performance for Large Firmware Deployments 8

USB Music on Hold Fixed Audio Adapter is not Supported 8

Call Treatment When No Path Is Available Default Parameter Change 8

Failover Interoperability with Cisco Jabber Clients 8
Devices Reset with Certificate Regeneration 9
MGCP IOS Gateway From PSTN Does Not Support Connected Address in ISDN Notify 9
Perfect Forward Secrecy is not Supported in IPsec Configuration 9
Change Perfmon Counter File Size Parameters in RTMT 9
HTTP/1.0 Not Supported On Cisco Unified IP Phone 7936 9
OS Admin Account Required for CLI-Initiated IM and Presence Upgrades 10

CHAPTER 3 Caveats 11
Bug Fixes and Updates 11
Bug Search Tool 11
Resolved Caveats 12
Open Caveats 12
Open Caveats for Unified Communications Manager Release 10.0(1) 13
Open Caveats for IM and Presence Service Release 10.0(1) 20

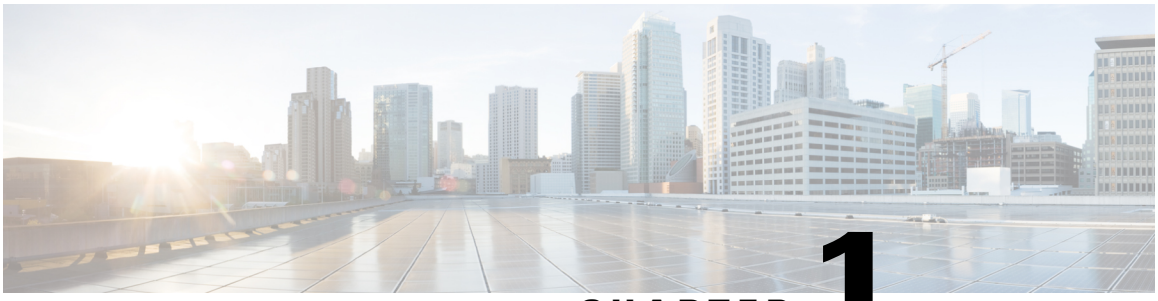
CHAPTER 4 Documentation Updates 23
Administration Guide 24
Cisco Unified IP Phone setup Description Character Length 24
Correction in Software Conference Bridge Maximum Audio Streams 24
Directory Number Field Description Updated 24
Directory Number Line Behavior in Cisco Unified Communications Manager 24
Disable Early Media on 180 Correction 25
Extension Mobility Now Supports Device Owners 25
Hostname and IP Address Field Can Contain a Fully Qualified Domain Name 25
Hostnames in IPv4 and IPv6 Environments 25
Hub_None Location Correction 25
ILS Restictions for Directory URIs 26
Incorrect Information about Deleting Route Patterns 26
Incorrect Note about User Locales 26
Incorrect Time Period Example 27
Insufficient Information about Call Control Agent Profile Fields 27
Line Group Deletion Correction 28
Maximum Hunt Timer Restriction 28

Missing Information for Allow Multiple Codecs in Answer SDP 28
Phone Support for Multilevel Precedence and Preemption 29
Service Profiles and Device Owner User IDs 29
Shared Lines May Reset Together 29
Time Is Not Manually Configurable 29
Transmit UTF8 for Calling Party Name Field Correction 30
UDS in Remote Cluster Service Configuration is Not Supported 30
LDAP Authentication Correction 30
A Server Restart is Required After Uploading a Certificate 31
Bulk Administration Guide 31
Bulk Administration Character Length 31
EMCC Device Calculation in the Bulk Administration Tool 31
Call Detail Records Administration Guide 32
Call Recording Section of CDR Examples 32
FAC and CMC Code is not Captured in CDR 33
Changing IP Address and Hostname 36
Additional Prerequisite for IP and Hostname Change on IM and Presence Service 36
Change IP Address or Hostname Using Unified Operating System GUI 36
CLI Reference Guide 37
Enable or Disable FIPS for IM and Presence Service 37
set network domain Conflicting Information 37
Show perf query counter Command Output 37
Support Removed for utils vmtools status 38
Compatibility Matrix 38
Missing Information About Supported ISR Gateways 38
Direct Upgrade from 7.1 to 10.0 is not Supported 38
Disaster Recovery System Guide 38
Supported SFTP Servers 38
Features and Services Guide 39
Calling Party Normalization Restriction 39
Call Queuing Update 40
Cisco Unified Communications Manager Sends INVITE Message to VCS 40
Client Matter Codes and Force Authorization Codes Not Supported on Cisco Jabber 40
Client Matter Codes, Forced Authorization Codes, and Failover Calls 40
Corrected License Report Update Interval 40

Force Authorization Codes Not Supported on Cisco Jabber 41
Gateway Recording Support 41
Incorrect Report for Device Mobility 41
Jabber Devices Count as Registered Devices 41
MGCP FXS Ports Do Not Require a License 41
Music On Hold and Native Call Queuing Behavior 42
Remote Destination and Auto Answer 42
Restart Intercluster Lookup Service 42
SAML SSO Authentication LDAP Attribute for User ID Setting 42
Video Capabilities and Enhanced Location Call Admission Control 42
Phone Displaying To Conference 43
Call Pickup Restriction 43
Installing Cisco Unified Communications Manager 43
Installation Warnings 43
JTAPI Developers Guide 44
MeetMe: Unsupported JTAPI Feature 44
Managed Services Guide 44
SNMP Limits 44
Unified Communications Manager Alarms 44
Online Help for Cisco Unified Communications Manager 45
Backup Device Limit Incorrect in Disaster Recovery System Online Help 45
Incorrect Description for Destination Number 45
Directory Number Field Description Updated 45
Remote Destination Configuration Page In the OLH Needs To Be Updated 45
OS Administration Guide 46
Time Is Not Manually Configurable 46
Add CA Signed CAPF Root Certificate to Trust Store 46
Real-Time Monitoring Tool Guide 47
Analyze Call Path Tool does not Work with Non-English Language 47
Incorrect Default Value for LogPartitionLowWaterMarkExceeded Alert 47
Incorrect Minimum Rate for Monitoring a Performance Counter 47
LowAvailableVirtualMemory Threshold Value is Incorrect 47
Security Guide 48
BAT User Template Accepts Only Hexadecimal Characters 48
IP Phone SSL VPN not Supported on Third Party Firewalls 48

MGCP FXS Ports Do Not Require a License 48
Replace ASA Certificate on AnyConnect VPN Phone 48
Secure and Nonsecure Indication Tone 49
CSCup54818 Support for CA Certificates in Mixed Mode 49
Enable Password Persistence 50
Resync Bandwidth Option is Removed 50
CNF File Encryption Is Not Supported by Default on 6901 and 6911, Cisco IP Phones 50
ITL File Size Limitation 50
Serviceability Guide 51
AXL Web Service Requirement for ICSA HA 51
Cisco CAR DB Service 51
Cisco Certificate Change Notification Service 51
Cisco IP Phone Service Removed from CM Services 52
Cisco SOAP-CallRecord Service 52
SNMP Limits 52
IM and Presence Security Best Practice 52
SOAP-Diagnostic Portal Database Service 52
Error in SYSLOG-MIB Parameters 53
System Guide 53
Call Transfer to Hunt Pilot Restriction 53
Email IDs on the Active Directory Server 53
LDAP Directory Support 53
Bandwidth Calculations 54
Insufficient Information About Third-Party Restrictions 54
Time of Day routing not Implemented for Message Waiting Indicator 54
TCP and UDP Port Usage Guide 55
Intercluster Lookup Service Name Correction 55
Missing Information about TCP Port 22 55
Missing Information about TCP Port 5555 55
Missing Information about Common Service Port 8006 56
Upgrade Guide 56
Disable or Postpone LDAP Synchronization During an Upgrade 56
Unified CM 10.0 Upgrade Process Correction 56
InterCluster Peer-User and Admin-CUMA Application User Roles Deprecated 56

Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service 57
Domain Name Change for Cisco Unified Communications Manager 57
Update Domain Name for Cisco Unified Communications Manager 57
Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager 58
Retrieve Chat Rooms on a Replaced Node 58



CHAPTER 1

Introduction

- About Release Notes, page 1
- Documentation for Release 10.0(1), page 2
- New and Changed, page 2
- Upgrades, page 2

About Release Notes

These release notes describe new features, requirements, restrictions, and caveats for Cisco Unified Communications Manager and IM and Presence Service. These release notes are updated for every maintenance release but not for patches or hot fixes.

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, VoIP gateways, mobile devices, and multimedia applications.

IM and Presence Service collects information about user availability, such as whether users are using communications devices (for example, a phone) at a particular time. IM and Presence Service can also collect information about individual user communication capabilities, such as whether web collaboration or video conferencing is enabled. Applications such as Cisco Jabber and Unified Communications Manager use this information to improve productivity among employees, that is, to help employees connect with colleagues more efficiently and determine the most effective way for collaborative communication.

Note In the past, export licenses, government regulations, and import restrictions have limited the ability of Cisco to supply Unified Communications Manager and IM and Presence Service worldwide. Cisco has obtained an unrestricted U.S. export classification to address this issue; IM and Presence Service Release 10.0(1) supports an export unrestricted (XU) version only. The unrestricted version differs from previous releases of IM and Presence Service in that it does not contain strong encryption capabilities.

Be aware that after you install an unrestricted release, you can never upgrade to a restricted version. You are not allowed to perform a fresh installation of a restricted version on a system that contains an unrestricted version.

Documentation for Release 10.0(1)

For complete information about this release, refer first to these Release Notes and then refer to the *Documentation Guide for Cisco Unified Communications Manager and IM and Presence Service* at the following URL:

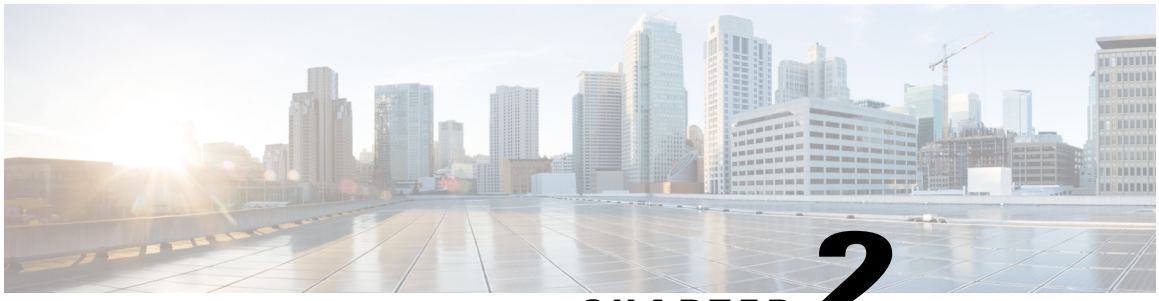
http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/docguide/10_0_1/CUCM_BK_C08E97F6_00_cucm-doc-guide-1001.html.

New and Changed

For information about New and Changed features in this release, see http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html.

Upgrades

For information about upgrading, as well as requirements for hardware and software, see http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html.



CHAPTER 2

Important Notes

- Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets, page 4
- Cisco Unified Mobility Disclaimer, page 4
- Deployment, page 4
- No Configuration During Upgrades, page 4
- Upgrade Considerations for Virtual Machines, page 5
- Upgrades from IM and Presence Service 10.0(1) Export Unrestricted, page 5
- Upgrade Fails if AXL Password Contains Special Characters, page 5
- Directory Search in Self Care, page 5
- DRS Restore of Failed IM and Presence Service Database Publisher Node Requires DRS Restore of Cisco Unified Communications Manager Publisher Node, page 6
- IP Phone SSL VPN not Supported on Third Party Firewalls, page 6
- Increase in Number of LDAP Sync Agreements, page 6
- Jabber Certificate Warnings with IM and Presence Service, page 6
- Parameter Settings, page 7
- Removal of Simplified Messaging Desk Interface (SMDI) and Music-On-Hold Live-Audio Source, page 7
- Self Care Breaks User Call Fwd Settings, page 7
- Self Care Portal Does Not Recognize the Default Voicemail Profile or Pilot, page 8
- TFTP Server Performance for Large Firmware Deployments, page 8
- USB Music on Hold Fixed Audio Adapter is not Supported, page 8
- Call Treatment When No Path Is Available Default Parameter Change, page 8
- Failover Interoperability with Cisco Jabber Clients, page 8
- Devices Reset with Certificate Regeneration, page 9
- MGCP IOS Gateway From PSTN Does Not Support Connected Address in ISDN Notify , page 9

- Perfect Forward Secrecy is not Supported in IPsec Configuration, page 9
- Change Perfmon Counter File Size Parameters in RTMT, page 9
- HTTP/1.0 Not Supported On Cisco Unified IP Phone 7936 , page 9
- OS Admin Account Required for CLI-Initiated IM and Presence Upgrades, page 10

Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets

This information applies to CSCtn79567.

Cisco Unified IP Phones 7940 and 7960 do not support Cisco-signed Java Midlets, but they can parse the service information from the phone configuration file.

Cisco Unified Mobility Disclaimer

Caution The Cisco Mobility solution is verified with only Cisco equipment. This solution may also work with other third-party PSTN gateways and Session Border Controllers (SBCs), but each Cisco Mobility feature is not guaranteed to work as expected.

If you are using this solution with third-party PSTN gateways or SBCs, Cisco technical support may not be able to resolve problems that you encounter.

Deployment

In Release 10.0(1) and later, Cisco only supports virtualized deployments of Cisco Unified Communications Manager (Unified Communications Manager) on Cisco Unified Computing System servers, or on a Cisco-approved third-party server configuration. In Release 10.0(1) and later, Cisco does not support deployments of Unified Communications Manager on Cisco Media Convergence Server servers.

Tape device is not supported in virtualized deployments. Upgrade to 10.0(1) and later removes the devices/schedules configured with tape device. Ensure to add the network device(if it does not exists) and re-configure the schedule for backup/restore post upgrade.

For more information about the deployment of Unified Communications Manager in a virtualized environment, see:

http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment.

No Configuration During Upgrades

Do not perform any configuration tasks during the upgrade process.

Caution If you are upgrading both Cisco Unified Communications Manager and IM and Presence Service, do not modify any of the IM and Presence Service server entries on the Application Server or Server configuration pages of the Cisco Unified CM Administration interface. The IM and Presence Service upgrade process automatically updates these entries on the Cisco Unified Communications Manager cluster during the final stages (switch version) of the upgrade process.

For upgrades from Release 8.x or 9.x to Release 10.x or later, any manual modification of these entries during the upgrade process will result in data migration failures between IM and Presence Service and Cisco Unified Communications Manager. If such failures occur, you must restart the entire upgrade process for both Cisco Unified Communcations Manager and IM and Presence Service clusters.

Upgrade Considerations for Virtual Machines

You must change the network adaptor type when upgrading a virtual machine. Follow the procedure in Section 5 in the Readme associated with the CUCM 10.0(1) OVA file download.

Not following the procedure can cause performance degradation, and result in a unsupported configuration.

Upgrades from IM and Presence Service 10.0(1) Export Unrestricted

If you are upgrading from IM and Presence Service 10.0(1) Export Unrestricted to any higher release of IM and Presence Service Export Unrestricted (including Service Updates), you must install the unrestricted upgrade COP file before you begin the upgrade: `ciscocm.cup.unrst_upgrade_10_0_1_vx.x.cop.sgn`. You can download this file from Cisco.com.

Upgrade Fails if AXL Password Contains Special Characters

This document update resolves CSCur00547.

If you have special characters in your Cisco Unified Communications Manager default administrative password, when you upgrade from releases 8.x or 9.x, the connection between IM and Presence Service and Cisco Unified Communications Manager fails. Before you upgrade from an 8.x or 9.x release, you must change your password so that all special characters are removed.

Directory Search in Self Care

The Directory Search option under User Options in releases before 10.0(1) has been removed from the 10.0(1) release onward. However, in the Self Care Portal, the same search capability is available under Contacts and Speed Dials, both of which a user can manually create.

DRS Restore of Failed IM and Presence Service Database Publisher Node Requires DRS Restore of Cisco Unified Communications Manager Publisher Node

This information applies to CSCuo02154.

If you need to perform a fresh install and a Disaster Recovery System (DRS) restore of a failed IM and Presence Service database publisher node, you must also perform a DRS restore of the Cisco Unified Communications Manager publisher node. There is a workaround for this issue which requires you to contact Cisco TAC for assistance.

Workaround

This workaround only applies if you have a backup of the IM and Presence Service database publisher node.

1. Insert the IM and Presence Service domain into the CUCM secureconfig table. You must conatct Cisco TAC for assistance with this step.
2. Reinstall the IM and Presence Service database publisher node.
3. Restore the IM and Presence Service database publisher node using the backup.
4. Resintall the IM and Presence Service subscriber nodes.
5. Restore the IM and Presence Service subscriber nodes.

IP Phone SSL VPN not Supported on Third Party Firewalls

This information applies to CSCun49156.

For IP Phones that use SSL VPN, third-party firewalls are not supported.

Increase in Number of LDAP Sync Agreements

This information applies to CSCul20279.

The maximum number of users that can be synced into a cluster is 160,000. This is the user limit for LDAP synchronization. The maximum number of LDAP sync agreements is 20. However, using 20 LDAP sync agreements with 160,000 users simultaneously is not supported. We recommend that the sync agreements for 160,000 users is 10 or less. 20 sync agreements is recommended only for a system for which the number of sync users is less than 80,000.

The initial LDAP synchronization times increase substantially (multiple hours) as the number of users and the number of sync agreements increase. Subsequent LDAP syncs will not take as long. If custom LDAP attributes are used, the synchronization time may increase and potentially double.

Jabber Certificate Warnings with IM and Presence Service

This information applies to CSCum63324.

When using the Cisco Jabber client, certificate warning messages can be encountered if the IP address is configured as the IM and Presence Service node name. To prevent Cisco Jabber from generating certificate warning messages, the FQDN should be used as the node name.

Parameter Settings

With the merging of Cisco Unified Communications Manager and IM and Presence Service, enterprise and service parameters are now shared between nodes in a cluster. As such, both types of nodes use the same settings for enterprise and cluster-wide parameters. You need to be aware that not all parameter settings are retained during an upgrade to Release 10.0(1). All enterprise parameters and cluster-wide service parameters that are common to both Cisco Unified Communications Manager and IM and Presence Service retain the value specified on Cisco Unified Communications Manager only, with one exception. The User Assignment Mode parameter is the only enterprise parameter that is retained during upgrade. Service parameters that apply to IM and Presence only are retained after an upgrade.

Cisco recommends that before you begin an upgrade, you make a note of parameter settings and evaluate the best settings for the combined cluster. This will allow you to easily configure those settings after the upgrade is complete.

Removal of Simplified Messaging Desk Interface (SMDI) and Music-On-Hold Live-Audio Source

The Simplified Messaging Desk Interface (SMDI) and Music-on-Hold Live-audio source as used by CMI and SME depend on bare metal USB support. Because this release is virtual-only, SMDI and Music-on-Hold Live-audio source are no longer supported.

Self Care Breaks User Call Fwd Settings

This information applies to CSCul90262.

Selecting the **Forward all calls to:** option in the Self Care Portal overwrites any configured **Advanced calling rules**. **Advanced calling rules** affect **Call Forward No Answer** and **Call Forward Busy** settings. You must reconfigure **Advanced calling rules** if you enable **Forward all calls to:** outside of the Self Care Portal, such as on a phone app.

The **Show Call Forwarding** option found in the System Enterprise parameters impact this issue as follows:

- If the parameter is set to "Show Only Forward All," the user cannot correct the defect by using the Advanced Calling Rules section, as it is not available.
- Customers can avoid end-users triggering this problem by hiding the **Call Forward settings** from the Self Care Portal by setting the "Show Call Forwarding" Enterprise Parameter to "Hide All Settings".

Self Care Portal Does Not Recognize the Default Voicemail Profile or Pilot

This information applies to CSCul51014.

If the voicemail profile is configured for directory numbers to inherit the system default, a message appears in the user Self Care portal stating that voicemail pilot has not been configured, even when voicemail is available. To avoid this message, and to provide your users the functionality to launch a call to the Voicemail Pilot using WebDialer, explicitly configure a voicemail profile on each DN.

TFTP Server Performance for Large Firmware Deployments

This information applies to CSCul30613.

Because of increased firmware sizes for some devices, firmware downloads have the potential to timeout and not download successfully from the TFTP server when many devices are simultaneously attempting to download firmware. We recommend that you monitor the download progress through Unified RTMT to ensure that all devices sucessfully upgrade. Devices that experience a download timeout require that you restart the download process on the affected endpoints by issuing an Apply Config or Reset/Restart command through Cisco Unified CM Administration.

USB Music on Hold Fixed Audio Adapter is not Supported

This information applies to CSCun07952.

Cisco Unified Communications Manager Release 10.x does not support the USB Music On Hold fixed audio adapter. You can configure this adapter for use with the SRST router-based multicast Music On Hold. However, the USB adapter is not supported on Release 10.x for MOH audio input from an external sound device, such as an SAT receiver or a CD/DVD. This loss of support may affect you if you use the USB Music On Hold fixed audio adapter and are upgrading from Unified Communications Manager Releases 7.x, 8.x, or 9.x.

Call Treatment When No Path Is Available Default Parameter Change

This information applies to CSCui70893.

In Release 10.0(1), the Location Bandwidth Manager service parameter “CallTreatmentWhenNoPathIsAvailable” default value of "reject call" has been changed to “allow call.” This change has been implemented to allow calls to proceed when a local hub is not functioning.

Failover Interoperability with Cisco Jabber Clients

If you have configured redundancy with backup servers, the following interoperability limitations apply to Cisco Jabber clients when the primary Cisco Unified Communications Manager server goes down:

- Softphone mode—If the Jabber client is in softphone mode, automatic failover is supported so long as the client has already downloaded the device information from the TFTP server (this occurs upon client startup). When the primary server goes down, the Call Preservation feature is invoked. All active Jabber calls are preserved, but users cannot invoke call-processing features. Once all preserved calls have ended, the Jabber client automatically switches over to the backup server. When the primary Cisco Unified Communications Manager server becomes available again, control reverts to the primary server.
- Deskphone mode—If the Jabber client is controlling a deskphone, automatic failover is not supported. However, you can switch over to the backup Cisco Unified Communications Manager server by signing out and signing in again on the Jabber client, or by switching to softphone mode, and then back to deskphone mode again.

Devices Reset with Certificate Regeneration

This information applies to CSCus63274.

All devices reset when you regenerate TVS, CCM, and CAPF client application certificates.

MGCP IOS Gateway From PSTN Does Not Support Connected Address in ISDN Notify

This information applies to CSCut08346.

The calling-line ID (CLID) information is not displayed through Media Gateway Control Protocol (MGCP) IOS gateway after the call is transferred since it does not support Connected Address in ISDN NOTIFY.

Perfect Forward Secrecy is not Supported in IPsec Configuration

This information applies to CSCuu74346.

Perfect Forward Secrecy (PFS) security service is not supported in IPsec configuration between Cisco Unified Communications Manager and Voice Gateway.

Change Perfmon Counter File Size Parameters in RTMT

If you have started logging perfmon counter data in RTMT and you want to change the file size and maximum number of files, you must first stop counter logging. After you stop the perfmon counters, you can make your changes and then restart perform counters.

HTTP/1.0 Not Supported On Cisco Unified IP Phone 7936

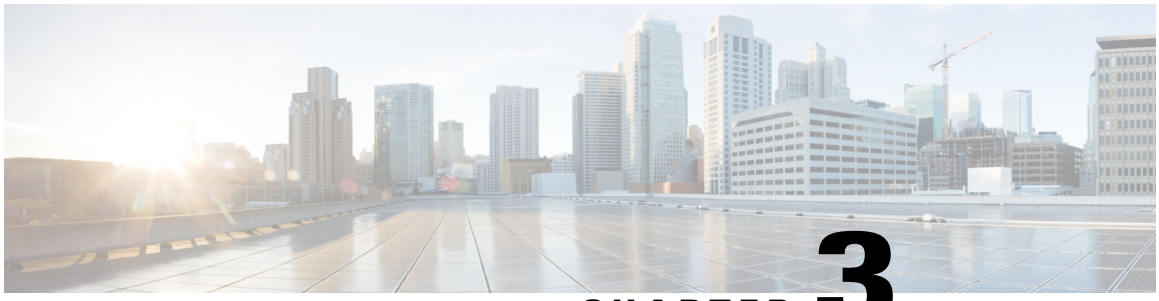
This information applies to CSCut80673.

HTTP/1.0 version is not supported on Cisco Unified IP Phone 7936 from Cisco Unified Communications Manager 10.x and later.

OS Admin Account Required for CLI-Initiated IM and Presence Upgrades

If you are using the **utils system upgrade** CLI command to upgrade IM and Presence Service nodes, you must use the default OS admin account, as opposed to a user with administrator privileges. Otherwise, the upgrade will not have the required privilege level to install essential services, thereby causing the upgrade to fail. You can confirm the account's privilege level by running the **show myself** CLI command. The account must have privilege level 4.

Please note that this limitation exists for CLI-initiated upgrades of IM and Presence Service only and does not apply to Cisco Unified Communications Manager. Also note that this limitation may be fixed for newer ISO files. Refer to your ISO Readme file for details on your specific ISO file. For up to date information on this limitation, see CSCvb14399 at https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvb14399.



CHAPTER 3

Caveats

- Bug Fixes and Updates, page 11
- Bug Search Tool, page 11
- Resolved Caveats, page 12
- Open Caveats, page 12

Bug Fixes and Updates

For the latest bug fixes, we recommend that you upgrade to Release 10.5(2).

Bug Search Tool

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
- All customer-found bugs

You can search for open and resolved caveats of any severity for any release using the Cisco Bug Search tool, an online tool available for customers to query defects according to their own needs.

To access the Cisco Bug Search tool, you need the following items:

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

Follow these steps to use Cisco Bug Search tool:

1. Access the Cisco Bug Search tool: https://tools.cisco.com/bugsearch/.
2. Log in with your Cisco.com user ID and password.

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

Tip Click **Help** on the Bug Search page for information about how to search for bugs, create saved searches, and create bug groups.

Resolved Caveats

You can find the latest resolved caveat information for Unified Communications Manager and IM and Presence Service by using the Bug Search tool, an online tool available for customers to query defects according to their own needs.

Tip

- You need an account with Cisco.com to use the Bug Search tool to find open and resolved caveats of any severity for any release.
- You can search for Unified Communications Manager and IM and Presence Service by selecting "Model/SW Family" in the **Product** drop-down list, and entering "Cisco Unified Communications" or "Cisco Unified Communications Manager IM & Presence Service", and allowing the Bug Search Tool to suggest products.

Related Topics

https://tools.cisco.com/bugsearch/

Open Caveats

The following sections describe possible unexpected behaviors in Unified Communications Manager and IM and Presence Service Release 10.0(1).

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

How to Interpret the Fixed-In Field in the Online Defect Record

When you open the online record for a defect, you see data in the "Fixed-In" field. The information that displays in this field identifies the list of interim versions in which the defect was fixed. These interim versions are then integrated into Unified Communications Manager or IM and Presence 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 maintenance releases may not be as clearly identified.

The following examples show how to decode the maintenance release interim version information. These examples show the format of the interim version along with the corresponding Unified Communications

Manager release that includes that interim version. Use these examples as guidance to better understand the presentation of information in these fields.

- 8.0(2.40000-x) = Cisco Unified Communications Manager 8.0(2c)
- 7.1(5.10000-x) = Cisco Unified Communications Manager 7.1(5)
- 7.1(3.30000-x) = Cisco Unified Communications Manager 7.1(3b)
- 7.1(3.20000-x) = Cisco Unified Communications Manager 7.1(3a)
- 7.1(3.10000-x) = Cisco Unified Communications Manager 7.1(3)
- 7.1(2.30000-x) = Cisco Unified Communications Manager 7.1(2b)
- 7.1(2.20000-x) = Cisco Unified Communications Manager 7.1(2a)
- 7.1(2.10000-x) = Cisco Unified Communications Manager 7.1(2)

Note Because defect status continually changes, be aware that the open caveats summarized in the following sections are a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access the Bug Search tool.

Open Caveats for Unified Communications Manager Release 10.0(1)

Table 1: Open Caveats for Unified Communications Manager, Release 10.0(1)

Identifier	Severity	Component	Headline
CSCtt26508	2	backup-restore	Reoccurring event when backup is not scheduled or fails
CSCul63632	2	saml-sso	Unable to add DNS domain to Prime Collaboration Deployment instance
CSCul71689	2	cp-device-manager	Route Group Members being skipped and reporting as device down-8.x/9.x
CSCul72351	2	cp-digit-analysis	Publisher and Subscriber calls out of Sync on call manager
CSCul79413	2	tapisdk	Not able to open a secure provider
CSCul83786	2	ims	IMS not validating OAuth Tokens after 30 mins of recipt of first token
CSCul98516	2	media_str_app	G.729 MOH stops after working for awhile
CSCuj04136	3	cm-docs	Parked Call doesnot get reverted to the recipient in shared line

Identifier	Severity	Component	Headline
CSCug93527	3	directory	CUC searchs for column "customfield1" while trying to import from AD
CSCue21290	3	car	Unable to generate CDR Reports after performing a Refresh Upgrade
CSCue46456	3	cmui	Change RU status message on OS admin UI
CSCug93527	3	directory	CUC searchs for column "customfield1" while trying to import from AD
CSCul14111	3	saml-sso	SAML SSO: Disable clusterwide failing intermittently on 10.0.1.10000-7
CSCul57618	3	cp-cac	Calls are stuck in queue when transfer is invoked and LBM is deactivated
CSCul62368	3	cp-mobility	UCM don't respond "200 OK" to Jabber mobile client's register message
CSCuo71657	3	cp-sip-station	Transcoder not inserted when SIP phone codec locked for recording
CSCul63295	3	cp-sip-trunk	Glare condition in EX90-CUBE call results in extra mlines. Call drops.
CSCul63317	3	bps-bat	BAT location import requires additional configuration or else calls fail
CSCul63662	3	cli	PCD "set network dns primary" gives misleading licensing warning
CSCul63711	3	cmcti	DeviceClosed event reported for CTIPort/RP when App fails over too soon
CSCul63736	3	backup-restore	DRFFailure alarms seen even though backup reported success on history.
CSCul64682	3	voice-sipstack	SIP Phones joining video conference are disconnected when SME is down
CSCul65265	3	ims	Tomcat : HTTPS thread Deadlock caused by IMS Java library
CSCul66335	3	elm	PLM should warn if license request attempted with dynamic MAC address
CSCul68681	3	cp-sip-station	URI is not xml encoded when sent in Conference Participant List

Identifier	Severity	Component	Headline
CSCul69464	3	ucmap	Discovery not working on some clusters
CSCul69849	3	ucmap	Discovery not working on some clusters
CSCul71661	3	ipma-service	Intercom line is not available on EM manager (RT Phones)
CSCul71876	3	ipma-service	IPMA service is not accessible on EM manager RT phone
CSCul73452	3	cp-mediacontrol	Not possible to open presentation channel
CSCul74017	3	cpi-os	Cannot view VMtools status from CLI unless VMtools ISO is mounted
CSCul74031	3	cpi-os	Cannot view VMtools status from CLI unless VMtools ISO is mounted
CSCul74047	3	cpi-os	VMtools require manual upgrade after any upgrade of IM/P version
CSCul78017	3	cp-sip-trunk	If srv used for destination on sip trunk the status is wrongly reported
CSCul63736	3	cmui	DRFFailure alarms seen even though backup reported success on history.
CSCuh96556	3	cpi-os	System Performance Impact During TCP Malformed Packet Flood
CSCui38773	3	cpi-mediacontrol	SIP Early <-> Early Media call leads to MXTimeOut
CSCui65827	3	cpi-cert-mgmt	Periodic CPU spike seen in system having large number of certificates
CSCui92275	3	cpi-third-party	VOS Platform - Need to update Struts for CVE patches
CSCuj14167	3	risdc	RTMT interface does not report perfmon counter on all nodes
CSCuj50309	3	saml-sso	Intermittent HTTP 500 error - SSO
CSCuj65125	2	cpi-os	"Cannot open Packages database..." error on console post L2 upgrade
CSCuj82211	3	cmcti	No Ringback to Remote Destination phone using Jabber Extend and Connect
CSCuj91148	3	cpi-os	UCM: Numerous Vulnerabilities in JDK 1.7.0_40

Identifier	Severity	Component	Headline
CSCuj96786	3	saml-sso	SAML SSO: Null Pointer Exception after disable saml sso in cureports
CSCul02171	3	cp-mediacontrol	H323, GW incorrectly sends OLC reject LCN 1 for the OLC already ACKed
CSCul13539	3	ucm-uct	Migration email is not internationalized
CSCul20716	3	cp-sip-station	High CPU and CodeYellow when Device registration exceed Max limit
CSCul24908	3	cp-mediacontrol	gen_keystore_pwd.sh Vulnerability allow escalation by pktCap_protectData
CSCul24917	3	cp-mediacontrol	Vulnerabilities in /etc/profile allow escalation via pktCap_protectData
CSCul25805	3	serv-soap	SOAP log collection service went down for few seconds
CSCul30604	3	cpi-appinstall	Issue with platform Administrator account creation if install is aborted
CSCul31400	3	cp-callcontrol	Call Failures due to leak in connection manager after redirection fails
CSCul38509	3	backup-restore	CUCM Backup failing due to interop issues with windows2008 and SMB
CSCul39029	3	cp-sip-trunk	V6 endpoints hold-resume call over V6-SIP-DO fail, if MOH not available
CSCul43710	3	ils	ILS to stop updating remoteuripattern table if replication is restarted
CSCul44464	3	backup-restore	DRS Backups fail Intermittently with JSCH Exception
CSCul46005	3	cmui	ALL-LANG: CCMAdmin: User/Phone Add settings are not displayed correctly
CSCul47405	3	cp-sip-trunk	CUCM does not re-send INVITE after receiving 422 following a 180
CSCul47655	3	cp-callqueuing	Dequeue call uses calling search space original calling party
CSCul51170	3	ccm-serviceability	Cisco CDP Module not loading correctly
CSCul51265	3	database	CUCM is not syncing DirectoryURI data after upgrade from 8.6.2

Identifier	Severity	Component	Headline
CSCul53246	3	cmui	MOH media resources not load balancing within the same MRG
CSCul53810	3	cp-unknown	CUCM Table Dump Entries and Size Not Accurate
CSCul54513	3	cp-ss-callback	CallBack phone alert displays wrong time formatCM 9
CSCul55637	3	cpi-appinstall	VM reset while RU in progress hampers subsequent RU upgrades
CSCul56397	3	cpi-os	Red Hat Enterprise Linux 6 Kernel Update to Address Numerous Vuls
CSCul56604	3	cpi-os	Python Hostname Check bypassing Vulnerability in SSL Module
CSCul59308	3	serv-web-pages	Quick User Phone Add Fails
CSCul64129	3	cm-docs	Parked Call doesnot get reverted to the recipient in shared line
CSCul81870	3	selinux	Sub Refresh upgrade blocked from 8.0.3
CSCul78735	3	selinux	VMTools Install Fails Due to SeLinux Blocking After Upgrade to 10.0.1
CSCul78742	3	elm	Update PLM OVA to use the vmxnet3 ethernet adapter
CSCul81003	3	cp-system	SDL signaling delay causes intermittent call failures
CSCul83453	3	backup-restore	CU IM & P Reporting is showing as 'nav.presence.report' on DRS Menu Page
CSCul84142	3	cmui	Assigned User Counts incorrect on CUCM Admin UI
CSCul84835	3	voice-sipstack	CUCM doesn't send ACK after 200 OK after receiving multiple PRACKs
CSCul86813	3	ipma-service	IPMA is not working on fresh Install
CSCul88594	3	cpi-os	Nss and NSPR DoS and Arbitrary Code Execution Vulnerabilitiees
CSCul88655	3	cmui	Spring Security Web Framework on UCM Vulnerable to Info Disclosure Vul
CSCul90746	3	dial_plan	Upgrade Fails to Migrate IDP Files with Many IDP Subdirectories
CSCul92580	3	cp-sip-station	CUCM applies incorrect IP address in Contact header

Identifier	Severity	Component	Headline
CSCul97884	3	cpi-os	Libjpeg Information Leak (Read of Uninitialized Memory) Vulnerabiilty
CSCul98349	3	cp-mobility	call failures on Mobile clients over edge. contact header missing.
CSCul98442	3	cp-sip-trunk	Intermittent Failure in direct ICT e2eRSVP calls
CSCum03147	3	cp-mobility	SNR: When mobile phone not available call is not sent to VoiceMail
CSCum03753	3	backup-restore	DRS should not restore if domain name does not match
CSCum03842	3	media_str_app	RX Stream for reading wave file is not closed in mutual hold scenario
CSCum05290	3	cmui	pingExecute servlet allows unauthenticated access to ping command
CSCum05293	3	e911	E911 Proxy - Insufficient handling of SQL Exception
CSCum05296	3	e911	E911 Proxy - SQL Injections in RESTful service
CSCum05302	3	ext-mobility	Extension Mobility (EMApp) - Unauthenticated Blind SQL Injection
CSCum05313	3	em-database	Dangerous Use of SQL Queries in CMDatabase.java
CSCum05318	3	cp-mobility	CCMIVR - Unauthenticated Blind SQL Injection
CSCum05326	3	ipma-service	IPMA - Multiple Unauthenticated SQL Injections
CSCum05337	3	selinux	CUCM WAR files are available to unauthenticated users
CSCum05340	3	bat	Arbitrary File Download in ccmadmin BulkAdministration
CSCum05343	3	ipma-service	IPMA - Reflective XSS on Login Page
CSCum05347	3	ccm-serviceability	log4jinit Web App Could Allow Degradation of Service for CLI Users
CSCum05362	3	cp-resourcecontrol	Stuck IPVMS streams preventing Announcement changes for Native Queuing
CSCum06165	3	cp-mediacontrol	secured conf participant blind xfer,new participant has no audio

Identifier	Severity	Component	Headline
CSCum06291	3	cp-resourcecontrol	Multicast MOH reversing G729 codec to G711 codecs - media resource issue
CSCum13308	3	voice-sipstack	SIP ACKs for UDP retransmissions are sent to proxy instead of UAC
CSCum13565	3	cp-mobility	Adjust Standard SIP Profile for Mobile Devices with proper timer values
CSCum14496	3	cm-ucr-dod	Login Grace Time value doesn't get transferred after an upgrade
CSCum17185	3	risdc	Available MOH multicase resource retrieves different value than expected
CSCum18220	3	bps-bat	Incorrect Warning displayed when you delete Line Template
CSCum18572	3	cp-callcontrol	Last Redirect Number to Unity Connection
CSCum21162	3	cpi-appinstall	RU 8.5.1 to 9.1.2 failed,csv files not exported correctly
CSCum22214	3	cp-sip-trunk	CAR Conference Bridge Utilization report shows 0 percent for MCU bridge
CSCum22654	3	backup-restore	Finesse config data cannot be restored from subscriber in a DRS scenario
CSCum23796	3	bps-bat	Informix Error while updating MRGL or Route List through BAT Import
CSCum24620	3	cp-mobility	In a SNR setup the digits are not sent out correctly
CSCum29912	3	cp-supple -mentary services	GW Recording failing when SIP Trunk is active on multiple nodes
CSCum35764	3	cmcti	get timeout response when start recording on chaperone device
CSCum36543	3	cmui	[Reg] IE 9 issue on Universal Line Template page/Universal Line Template
CSCum37479	3	cpi-os	Cluster Manager floods S1 Alarm for nodes in INITIATOR state
CSCum37667	3	cpi-os	CLM: list_cluster.sh converts host names to lower case format

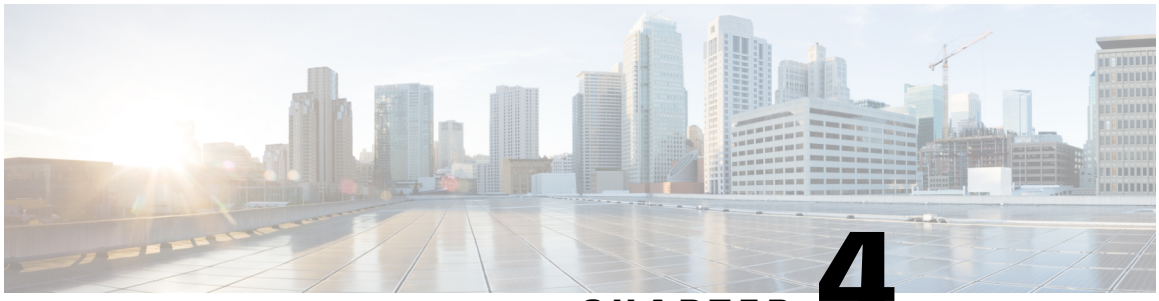
Identifier	Severity	Component	Headline
CSCum38792	3	cpi-os	Pixman Remote Denial of Service Vulnerability (CVE-2013-6425)
CSCum38798	3	cpi-os	CA Mis-Issued Certificate Could Allow Man-In-The-Middle Attacks
CSCum39811	3	ucmap	PCD/UCMAP does not display Discovering in discovery status
CSCum40689	3	trace-library	CUCM calllogs missing out leg messages between CUCM & EP

Open Caveats for IM and Presence Service Release 10.0(1)

The following table lists open caveats that may cause unexpected behavior in the latest IM and Presence Service release. These caveats may also be open in previous releases. Bugs are listed in alphabetical order by component and then in numerical order by severity.

Identifier	Severity	Component	Headline
CSCum00560	3	xcp-textconf	A group chat participant cannot change to being a hidden user
CSCum43132	3	xcp-textconf	TC service leaks memory when third-party compliance is enabled
CSCul80286	3	xcp-jsm	Temp buddy presence can not be updated
CSCto56517	3	xcp-textconf	XCP Text Conference Manager Core Dump
CSCuj48155	3	xcp-router	IM&P - Expected error delivery message not sent to Jabber
CSCul27793	3	xcp-router	"Unknown Error" when restarting the XCP Router service
CSCul66300	3	sync-agent	Cisco Sync Agent hangs after fresh install and doesn't process CN's
CSCul53463	3	security	Third party XMPP clients cannot login when LDAP SSL auth is enabled
CSCul22204	3	vos	VM tools update via CLI requires a manual reboot to complete
CSCuf65811	3	srm	SRM HA failover parameters are not sized for fully used OVA by default
CSCug71816	3	srm	IMP Pub can become stuck in initializing state after server shutdown

Identifier	Severity	Component	Headline
CSCug76766	3	epe	DND is incorrect cascading to a device with a shared line appearance
CSCuh64518	3	epe	CUP: Presence Engine Coredump during IM & Presence server restart.
CSCui09350	3	xcp-jsm	Jabber iphone, custom status text lost when place in background
CSCuj63130	3	database	Federation Routing IM/P FQDN can be corrupted in PCD network migration
CSCuj65779	3	epe	User Rename, Move & Assignment operations fails if server is failed over
CSCuj69195	3	epe	When user clicks on "click to call", sip proxy cores, RCC with MOC
CSCuj91178	3	gui	Assigned User Counts include User Templates on CUCM IM & Presence
CSCul05066	3	gui	CUC page on CUP redirects to CUCM hostname rather than CUCM IP address
CSCul11123	3	database-ids	UC Voicemail supported characters mismatching UC Service supported chars
CSCul18330	3	srm	SRM status return to Normal/Normal before JSM sessions are moved
CSCul30258	3	func-test	SIP Proxy cores when invalid RouteEmbedTemplate parameter set
CSCuh25203	3	gui-admin	HA error message displayed incorrectly on a single node cluster



CHAPTER 4

Documentation Updates

- Administration Guide, page 24
- Bulk Administration Guide, page 31
- Call Detail Records Administration Guide, page 32
- Changing IP Address and Hostname, page 36
- CLI Reference Guide, page 37
- Compatibility Matrix, page 38
- Disaster Recovery System Guide, page 38
- Features and Services Guide, page 39
- Installing Cisco Unified Communications Manager, page 43
- JTAPI Developers Guide, page 44
- Managed Services Guide, page 44
- Online Help for Cisco Unified Communications Manager, page 45
- OS Administration Guide, page 46
- Real-Time Monitoring Tool Guide, page 47
- Security Guide, page 48
- Serviceability Guide, page 51
- System Guide, page 53
- TCP and UDP Port Usage Guide, page 55
- Upgrade Guide, page 56
- Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service, page 57
- Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager, page 58

Administration Guide

Cisco Unified IP Phone setup Description Character Length

This documentation update resolves CSCut08307.

The character length for the **Description** field is incorrect in the *Cisco Unified Communications Manager Administration Guide*. The following table shows the correct description.

Field	Description
Description	Identify the purpose of the device. You can enter the user name (such as John Smith) or the phone location (such as Lobby) in this field. For Cisco VG248 gateways, begin the description with`VGC<mac address>`. The description can include up to 128 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Correction in Software Conference Bridge Maximum Audio Streams

This documentation update resolves CSCuu44805.

The maximum audio streams per software conference bridge is incorrectly listed as 128 in the “Software Conference Devices” section of the *Cisco Unified Communications Manager Administration Guide*. The correct value is 256.

Directory Number Field Description Updated

This documentation update resolves CSCur86259.

The following information is omitted from the “Directory Number Settings” topic in the Cisco Unified Communications Manager Administration Guide and online help:

The Directory Number is a mandatory field.

Directory Number Line Behavior in Cisco Unified Communications Manager

This documentation update resolves CSCuo74599.

The following information is omitted in the “Set Up Cisco Unified IP Phone” procedure in the *Cisco Unified Communications Manager Administration Guide*:

After you add a directory number to a phone and click **Save**, the following message appears:

```
Directory Number Configuration has refreshed due to a directory number
change. Please click Save button to save the configuration.
```

Disable Early Media on 180 Correction

This documentation update resolves CSCup68350.

The "SIP Profile Settings" section in the *Administration Guide* contains incorrect information about the **Disable Early Media on 180** check box. The description states that the setting applies to both the 180 and 183 responses, but the setting applies to only the 180 response.

Extension Mobility Now Supports Device Owners

This documentation update resolves CSCun04965.

You can now configure the Owner User ID in the Phone Settings interface if you are using Extension Mobility. Extension Mobility now supports device owners. A note indicating otherwise is listed in error in the *Cisco Unified Communications Manager Administration Guide*.

Hostname and IP Address Field Can Contain a Fully Qualified Domain Name

This documentation update resolves CSCur62680.

The following information is omitted from the **Host Name/IP Address** field description, listed under the "Server Setup" chapter in the *Administration Guide* and the online help.

You can also enter a fully qualified domain name (FQDN) in this field—for example, `cucmname.example.com`.

Note If Jabber clients are used, we recommend that you use an FQDN instead of a hostname so that the Jabber clients can resolve the Unified Communications Manager domain name.

Hostnames in IPv4 and IPv6 Environments

This documentation update resolves CSCun74975.

The following information is omitted from the **IPv6 Address (for dual IPv4/IPv6)** field description under "Server Settings" in the *Cisco Unified Communications Manager Administration Guide*:

You cannot use an IPv4 address as a hostname in a network environment with both IPv4 and IPv6 addresses.

Hub_None Location Correction

This documentation update resolves CSCuu40700.

The "Location" chapter in the *Administration Guide* and online help states that " The Hub_None location specifies unlimited audio bandwidth and unlimited video bandwidth." This information is inacurrate. The correct information for Hub_None is as follows:

Hub_None is an example location that typically serves as a hub linking two or more locations. It is configured by default with unlimited intra-location bandwidth allocations for audio, video, and immersive bandwidth, but you can specify bandwidth allocations for each of these. By default, devices not assigned to other locations are assigned to Hub_None.

ILS Restictions for Directory URIs

This documentation update resolves CSCus74994.

The following information about Directory URIs has been added to the Directory number settings table in the *Cisco Unified Communications Manager Administration Guide*:

The maximum number of directory URIs that the Intracluster Lookup Service (ILS) can replicate is seven.

Incorrect Information about Deleting Route Patterns

The *Cisco Unified Communications Manager Administration Guide* and online help contain incorrect information about deleting route patterns such as route groups, hunt lists, and hunt pilots.

The following information further explains the context:

The association of any pattern or directory number (DN) to any device is separate from the devices and patterns themselves. As a result, you can delete a route list even if it is currently used for a route pattern. The same applies to hunt lists, hunt pilots, phones, and DNs.

As a best practice, whenever you remove a device, you must ensure that any associated pattern or DN is accounted for in your numbering plan. If you no longer need a pattern or DN, you must delete it separately from the device with which it was associated. Always check the configuration or dependency records before you delete a hunt list.

The following is an example of incorrect information in the guide:

Cisco Unified Communications Manager associates hunt lists with line groups and hunt pilots; however, deletion of line groups and hunt pilots does not occur when the hunt list is deleted. To find out which hunt pilots are using the hunt list, click the Dependency Records link from the Hunt List Configuration window. If dependency records are not enabled for the system, the dependency records summary window displays a message.

The following is the corrected information:

Cisco Unified Communications Manager associates hunt lists with line groups and hunt pilots. You can delete a hunt list even when it is associated with line groups and hunt pilots. To find out which hunt pilots are using the hunt list, click the Dependency Records link from the Hunt List Configuration window. If dependency records are not enabled for the system, the dependency records summary window displays a message.

Incorrect Note about User Locales

This documentation update resolves CSCuq42434.

The note about user locales in the Cisco Unified IP Phone settings section of the *Administration Guide* incorrectly states that Cisco Unified Communications Manager uses the user locale that is association with the device pool. The following is the correct note:

Note If no user locale is specified, Cisco Unified Communications Manager uses the user locale that is associated with the common device configurations.

Incorrect Time Period Example

This documentation update resolves CSCvb74432.

The time period documentation contains an incorrect example that can cause configuration problems. It suggests to use a date range for a single day time period: "Choose a Year on value of Jan and 1 and an until value of Jan and 1 to specify January 1st as the only day during which this time period applies."

That is incorrect; please avoid using this example for the "Year on...until" option for time periods.

Insufficient Information about Call Control Agent Profile Fields

This documentation update resolves CSCuq11351.

The **Call Control Agent Profile** chapter in *Cisco Unified Communications Manager Administration Guide* contains insufficient information about the Call Control Agent Profile configuration fields. The following table contains the detailed information.

The following table describes the Call Control Agent Profile settings.

Table 2: Call Control Agent Profile Settings

Field	Description
Call Control Agent Profile Configuration	
Call Control Agent Profile ID	Enter a unique ID for the Call Control Agent Profile. This ID is associated with the Directory Number. It is a mandatory field. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), and space ( ).
Primary Softswitch ID	Enter the primary softswitch ID (prefix) of the directory number alias servers. It is a mandatory field. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), and space ( ).
Secondary Softswitch ID	Enter the secondary softswitch ID (suffix) of the directory number alias servers. The allowed values for this field are alphanumeric (a-zA-Z0-9), period (.), dash (-), and space ( ).
Object Class	Enter the object class name for the directory numbers associated with the call control agent profile. It is a mandatory field. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), and space ( ).
Subscriber Type	Enter the subscriber type of the directory numbers associated with the call control agent profile. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), space ( ), and at (@).

Field	Description
SIP Alias Suffix	Enter the SIP alias suffix. The E.164 number that you specify for the directory number is appended to this suffix when mapping to the SIP Alias field in the LDAP directory. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), space ( ), and at (@).
SIP User Name Suffix	Enter the SIP user name suffix. The E.164 number that you specify for the directory number is appended to this suffix when mapping to the SIP User Name field in the LDAP directory. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), space ( ), and at (@).

Line Group Deletion Correction

This documentation update resolves CSCuq26110.

The following is a correction to Line Group Deletion.

You can delete a line group that one or more route/hunt lists references. If you try to delete a line group that is in use, Cisco Unified Communications Manager displays an error message.

Tip Dependency Records is not supported for line groups. As a best practice, always check the configuration before you delete a line group.

Maximum Hunt Timer Restriction

This documentation update resolves CSCuo90637.

The following note is omitted from the *Cisco Unified Communications Manager Administration Guide* and online help for Hunt Group configuration:

Caution Do not specify the same value for the Maximum Hunt Timer and the RNA Reversion Timeout on the associated line group.

Missing Information for Allow Multiple Codecs in Answer SDP

This documentation update resolves CSCup79162.

The following information is omitted from the "SIP Profile Settings" topic in the *Cisco Unified Communications Manager Administration Guide* and online help:

Configure **Allow multiple codecs in answer SDP** for the following:

- Third-party SIP endpoints that support this capability
- SIP trunks to third-party call controls servers that uniformly support this capability for all endpoints

Do not configure this capability for SIP intercluster trunks to Cisco SME or other Cisco Unified Communications Manager systems.

Phone Support for Multilevel Precedence and Preemption

This documentation update resolves CSCvb37715.

The restrictions in the Multilevel Precedence and Preemption (MLPP) chapter incorrectly state that only SCCP phones support this feature.

SCCP phones and some SIP phones support MLPP. To verify feature support, see the Cisco Unified IP phone administration guide for your model.

Service Profiles and Device Owner User IDs

This documentation update resolves CSCuu43939.

The following information is omitted from the "Service Profile Setup" chapter in the *Cisco Unified Communications Manager Administration Guide*:

A service profile is applied for a given device only when the owner user ID is specified. In that case, the service profile configured for the respective user is applied.

A note in the Service Profile Settings table is incorrect. The correct note is:

Note If you specify a default service profile, end users that do not have an associated service profile automatically inherit the default service profile settings. In the same manner, any devices that do not have specified a owner user ID inherit the default service profile settings.

Shared Lines May Reset Together

This documentation update resolves CSCvb24186.

The phone reset tips in the "Cisco Unified IP Phone Setup" chapter do not state what happens when a shared directory number is added to a phone, or when the shared directory number's settings are updated.

This statement explains this scenario:

You do not have to reset a Cisco Unified IP Phone after you add a directory number or update its settings for your changes to take effect. Cisco Unified Communications Manager automatically performs the reset. In a shared line scenario, phones that have a shared line may reset when the shared directory number is added to another phone, or when those directory number settings are updated. You may reset a Cisco Unified IP Phone at any time by using the following procedure.

Time Is Not Manually Configurable

This information relates to CSCul67741.

The following note appears in the Cisco Unified OS Administration user interface in the **Settings** > **Time** menu and the *Cisco Unified OS Administration Guide*:

Note Before you can manually configure the server time, you must delete any NTP servers that you have configured.

Because it is mandatory to have at least one NTP server, this note is inaccurate. The following is the correct note:

Note You cannot configure time manually from the **Time** window, because you cannot delete all NTP servers and one NTP server is required.

Transmit UTF8 for Calling Party Name Field Correction

This documentation update resolves CSCup45037.

The *Cisco Unified Communications Manager Administrator Guide* specifies that the SIP trunk field **Transmit UTF-8 for Calling Party Name** uses the user locale setting of the device pool to determine what to send in the Calling Party Name field. However, the device pool does not have a user locale field. It has a network locale field, and both the Common Device Configuration record, and the Phone record itself have user locale fields.

The following is the process that the SIP trunk uses to obtain the user locale:

If the **Transmit UTF-8 for Calling Party Name** is checked to obtain the locale, the SIP trunk attempts to obtain the locale from the device. If that attempt fails, the SIP trunk attempts to obtain the user locale from the Common Device Configuration, and if that attempt fails, the SIP trunk obtains the user locale that is used for the Enterprise Parameters.

UDS in Remote Cluster Service Configuration is Not Supported

This documentation update resolves CSCuv67224.

In the “Remote Cluster Settings” table under topics related to advanced features, the content about the usage of the UDS check box is incorrect; even though a check box appears on the user interface under **Advanced Features** > **Cluster View**, the setting is not supported. User Data Service (UDS) is a service that is enabled by default.

LDAP Authentication Correction

This documentation update resolves CSCux00028.

The “Update LDAP Authentication ” section in the *Cisco Unified Communication Manager Administration Guide* contains incorrect information about “LDAP Authentication”. The description states that the LDAP synchronization must be disabled to make changes to the LDAP authentication settings. The correct information for “LDAP Authentication” is as follows:

LDAP synchronization must be enabled to make changes to the LDAP authentication settings.

A Server Restart is Required After Uploading a Certificate

This documentation update resolves CSCux67134.

The following is note omitted from the "Upload Certificate or Certificate Chain" chapter in the *Administration Guide* for Cisco Unified Communications Manager:

Note Restart the affected service after uploading the certificate. When the server comes back up you can access the CCMAdmin or CCMUser GUI to verify your newly added certificates in use.

Bulk Administration Guide

Bulk Administration Character Length

This documentation update resolves CSCum94975.

The character length for the **User Template Name** field is incorrect in the *Cisco Unified Communications Manager Bulk Administration Guide*. The following table shows the correct description.

Field	Description
User Template Name	Enter a unique name, up to 132 alphanumeric characters, for the user template.

EMCC Device Calculation in the Bulk Administration Tool

This documentation update resolves CSCuy38765.

The following information is omitted from the "Insert EMCC Devices" procedure in the *Bulk Administration Guide*:

To determine how many EMCC devices to add, look at the number of registered phones and add 5% to account for devices that may not be registered at the moment. If you have 100 phones, multiply 100 by 0.5, which equals 5. You add the result (5) to the total (100). The number of EMCC devices is 105.

To display information about the number of registered phones, gateways, and media resource devices on Cisco Unified Communications Manager, open RTMT and choose **Voice/Video > Device > Device Summary**.

Call Detail Records Administration Guide

Call Recording Section of CDR Examples

The Call Recording section of the CDR Examples chapter in the *Cisco Unified Communications Manager Call Detail Records Administration Guide* contains two call recording scenarios. However, the CDR examples that accompany the scenarios are monitoring CDRs. Following are the recording CDRs.

1 The customer (9728134987) calls the agent (30000), and the agent answers. The Recorder's DN is 90000. The recording feature creates two recording calls to the recording device, which results in two additional CDRs: one for the agent voice, and another for the customer voice. The origConversationID from the recording CDRs matches the destLegCallIdentifier of the recorded CDR. In this scenario, the customer hangs up.

Field Names	Recorded Call CDR	Recording Call CDR1	Recording Call CDR2
globalCallID_callId	7	10	11
origLegCallIdentifier	16777110	16777120	16777122
destLegCallIdentifier	16777111	16777121	16777123
callingPartyNumber	9728134987	BIB	BIB
originalCalledPartyNumber	30000	90000	90000
finalCalledPartyNumber	30000	90000	90000
lastRedirectDn	30000	90000	90000
origCause_Value	16	0	0
dest_CauseValue	0	0	0
origCalledPartyRedirectReason	0	354	354
lastRedirectRedirectOnBehalfOf	0	354	354
origCalledPartyRedirectOnBehalfOf		27	27
lastRedirectRedirectOnBehalfOf		27	27
origConversationID	0	16777111	16777111

2 The agent (30000) calls the customer (9728134987), and the customer answers. The Recorder's DN is 90000. The recording feature creates two recording calls to the recording device, which results in two additional CDRs: one for the agent voice, and another for the customer voice. The **origConversationID**

field from the recording CDRs will match the **origLegCallIdentifier** field of the recorded CDR. In this scenario, the agent hangs up.

Field Names	Recorded Call CDR	Recording Call CDR 1	Recording Call CDR 2
globalCallID_callId	71	100	110
origLegCallIdentifier	16777113	16777220	16777222
destLegCallIdentifier	16777114	16777221	16777223
callingPartyNumber	30000	BIB	BIB
originalCalledPartyNumber	9728134987	90000	90000
finalCalledPartyNumber	9728134987	90000	90000
lastRedirectDn	9728134987	90000	90000
origCause_Value	16	16	16
dest_CauseValue	0	0	0
origCalledPartyRedirectReason	0	354	354
lastRedirectRedirectOnBehalfOf	0	354	354
origCalledPartyRedirectOnBehalfOf		27	27
lastRedirectRedirectOnBehalfOf		27	27
origConversationID	0	16777113	16777113

FAC and CMC Code is not Captured in CDR

This documentation update resolves CSCus91749.

The following information about CDR entry for FAC and CMC calls is omitted in the Forced authorization code (FAC) and Client Matter Code (CMC) topic in the Cisco Unified Communications Manager Call Detail Records Administration Guide .

FAC

CDR will now be written for a setup call leg for all the unanswered calls before the call is redirected to another caller if FAC is used to setup the call.

Note This call will not have any connect time since media is not connected for this call. The CDR will be logged regardless of the service parameter **CdrLogCallsWithZeroDurationFlag** if FAC is present in the call.

FAC Example 2

Blind conference using FAC:

1. Call from 136201 to 136111.
2. 136111 answers and speaks for a few seconds.
3. 136201 presses the **Conference** softkey and dials 136203.
4. The user is prompted to enter the FAC code and the user enters 124. FAC code 124 is configured as level 1 and given a name as Forward_FAC.
5. While 136203 is ringing, 136201 presses the **Conference** softkey to complete the conference.
6. 136203 answers the call.
7. The three members in the conference talk for sometime.
8. 136111 hangs up, leaving 136201 and 136203 in the conference. Since there are only two participants in the conference, the conference feature will join these two directly together and they talk for a few seconds.

FieldNames	Orig Call CDR	Setup Call CDR	Conference CDR 1	Conference CDR 2	Conference CDR 3	Final CDR
globalCallID_callId	60015	60016	60015	60015	60015	60017
origLegCallIdentifier	23704372	23704374	23704373	23704372	23704376	23704377
destLegCallIdentifier	23704373	23704376	23704381	23704380	23704382	23704378
callingPartyNumber	136201	136201	136111	136201	136203	136201
origCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
finalCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
lastRedirectDn	136111	136203	136201	136201	136201	136203
origCause_Value	393216	0	16	393216	393216	0
dest_CauseValue	393216	0	393216	393216	393216	16
authCodeDescription		Forward_FAC				
authorizationLevel	0	1	0	0	0	0
Duration	18	0	37	37	32	38

FieldNames	Orig Call CDR	Setup Call CDR	Conference CDR 1	Conference CDR 2	Conference CDR 3	Final CDR
authorizationCode		124				

Note The setup call CDR for this example is generated even though it is of zero duration since FAC is used for this call.

CMC Example 2

Blind conference using CMC :

1. Call from 136201 to 136111.
2. 136111 answers and speaks for a few seconds.
3. 136201 presses the **Conference** softkey and dials 136203.
4. The user is prompted to enter the CMC code and the user enters 125. CMC code 125 is configured as level 1 and is given a name as Forward_CMC.
5. While 136203 is ringing, 136201 presses the **Conference** softkey to complete the conference.
6. 136203 answers the call.
7. The three members in the conference talk for sometime.
8. 136111 hangs sup, leaving 136201 and 136203 in the conference. Since there are only two participants in the conference, the conference feature will join these two directly together and they talk for a few seconds.

FieldNames	Orig Call CDR	Setup Call CDR	Conference CDR 1	Conference CDR 2	Conference CDR 3	Final CDR
globalCallID_callId	60025	60026	60025	60025	60025	60027
origLegCallIdentifier	23704522	23704524	23704523	23704522	23704526	23704527
destLegCallIdentifier	23704523	23704526	23704531	23704530	23704532	23704528
callingPartyNumber	136201	136201	136111	136201	136203	136201
origCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
finalCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
lastRedirectDn	136111	136203	136201	136201	136201	136203
origCause_Value	393216	0	16	393216	393216	0

FieldNames	Orig Call CDR	Setup Call CDR	Conference CDR 1	Conference CDR 2	Conference CDR 3	Final CDR
dest_CauseValue	393216	0	393216	393216	393216	16
authCodeDescription		Forward_CMC				
authorizationLevel	0	1	0	0	0	0
Duration	20	0	32	32	25	48
authorizationCode		125				

Note The setup call CDR for this example is generated even though it is of zero duration since CMC is used for this call.

Changing IP Address and Hostname

Additional Prerequisite for IP and Hostname Change on IM and Presence Service

This documentation update resolves CSCun73445.

Item Added to Pre-Change Task List

For each cluster where the publisher/subscriber node being changed is an intercluster peer, remove the publisher's/subscriber's cluster from the list of intercluster peers.

For example, ClusterA, ClusterB and ClusterC are all intercluster peers. You want to change the hostname on the publisher node of ClusterA. You must first remove the ClusterA publisher node from the list of intercluster peers on both ClusterB and ClusterC.

Change IP Address or Hostname Using Unified Operating System GUI

This documentation update resolves CSCvc70649.

The following information is omitted from the "IP Address and Hostname Changes" chapter in the *Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service*.

Changing the IP address or hostname triggers an automatic self-signed certificate regeneration. This causes all devices in the cluster to reset so that they can download an updated ITL file. If your cluster is using CA-signed certificates, you will need to have them re-signed.

CLI Reference Guide

Enable or Disable FIPS for IM and Presence Service

This documentation update resolves CSCuo56537.

Warning FIPS 140-2 mode for IM and Presence Service is pending certification at this time and is not supported until certification is complete.

Consider the following information before you enable or disable FIPS 140-2 mode for IM and Presence Service: After you enable or disable FIPS 140-2 mode for IM and Presence Service, the Tomcat certificate is regenerated and the node reboots. The Intercluster Sync Agent syncs the new Tomcat certificate across the cluster; this can take up to 30 minutes. Until the new Tomcat certificate is synced across the cluster, an IM and Presence Service subscriber node cannot access information from the IM and Presence Service database publisher node. For example, a user who is logged in to the Cisco Unified Serviceability GUI on a subscriber node cannot view services on the IM and Presence Service database publisher node. Users see the following error message until the synching is complete: `Connection to server cannot be established (certificate exception)`

set network domain Conflicting Information

This documentation update resolves CSCup03425.

The set network domain command section of the Set Commands chapter in the *Command Line Interface Guide for Cisco Unified Communications Solutions* contains conflicting information about manual and automatic certificate regeneration of all Cisco Unified Communications Manager certificates. At present, only automatic regeneration of certificates is supported.

The content related to manual certificate regeneration has been removed from the Usage Guidelines section. The following is the final content of the Usage Guidelines section:

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

Caution If you continue, this command causes a temporary loss of network connectivity.

Show perf query counter Command Output

This documentation update resolves CSCuo70238.

The following note is omitted from the **show perf query counter** command section in the *Cisco Unified Communications Command Line Interface Guide*.

Note The output that this command returns depends on the number of endpoints that is configured in the Route Groups in Cisco Unified Communications Manager.

Support Removed for utils vmtools status

The `utils vmtools status` CLI command is no longer supported. For VMware status, check the vSphere client instead.

Compatibility Matrix

Missing Information About Supported ISR Gateways

This documentation update resolves CSCur93869.

The following information is missing from the "ISR-G2 Gateways" topic in the *Compatibility Information for Cisco Unified Communications Manager Release 10.x*.

ISR Voice gateway series (Cisco 4431 and 4451).

Direct Upgrade from 7.1 to 10.0 is not Supported

This documentation update resolves CSCus62385

Direct upgrade using DMA from 7.1.5 to 10.0 is not supported; therefore 6.0x, 7.0x, 8.0x, and 8.5x versions were added under the Supported section and the information was deleted from the Direct upgrade section.

Disaster Recovery System Guide

Supported SFTP Servers

This documentation update resolves CSCur96680.

The following information is omitted from the *Disaster Recovery System Administration Guide*.

Note We recommend that you retest the DRS with your SFTP server after you upgrade your Unified Communications Manager, upgrade your SFTP server, or you switch to a different SFTP server. Perform this step to ensure that these components operate correctly together. As a best practice, perform a backup and restore on a standby or backup server.

Use the information in the following table to determine which SFTP server solution to use in your system.

Table 3: SFTP Server Information

SFTP Server	Information
SFTP Server on Cisco Prime Collaboration Deployment	This server is provided and tested by Cisco, and supported by Cisco TAC. Version compatibility depends on your version of Unified Communications Manager and Cisco Prime Collaboration Deployment. See the *Cisco Prime Collaboration Deployment Admin Guide* before you upgrade its version (SFTP) or Unified Communications Manager to ensure that the versions are compatible.
SFTP Server from a Technology Partner	These servers are third party provided, third party tested, and jointly supported by TAC and the Cisco vendor. Version compatibility depends on the third party test. See the Technology Partner page if you upgrade their SFTP product and/or upgrade UCM for which versions compatible: https://marketplace.cisco.com
SFTP Server from another Third Party	These servers are third party provided, have limited Cisco testing, and are not officially supported by Cisco TAC. Version compatibility is on a best effort basis to establish compatible SFTP versions and Unified Communications Manager versions. For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner.

Features and Services Guide

Calling Party Normalization Restriction

This documentation update resolves CSCuo56960.

The following restriction is omitted from the *Features and Services Guide for Cisco Unified Communications Manager*:

When calling or called party transformations are applied at the gateway or route list level, the calling number in the facility information element (IE) for QSIG calls is the post-transformation number. However, the called party in the facility IE is the pre-transformation called party number.

The calling party that is sent after transformation through the gateway is typically localized and does not cause an issue with the display and routing. The called party is typically the dialed digits and is displayed on the calling phone, so the transformation is not relayed for called party transformations. Called party transformation is designed to send the information based on the gateway that the call is going through, regardless of how the

number is dialed. Called party transformation is kept at the gateway level and not updated, whereas the calling party is updated.

Call Queuing Update

The Performance and Scalability topic in the Call Queuing chapter of the *Cisco Unified Communications Manager Features and Services Guide* contains a bullet that says that call queuing is not supported with broadcast algorithm hunt lists. This bullet point is incorrect and should be removed.

Cisco Unified Communications Manager Sends INVITE Message to VCS

This documentation update resolves CSCuv22205.

The following information is omitted from the “Cisco Unified Mobility” chapter:

When an enterprise user initiates a call from a remote destination to Cisco Jabber, Cisco Unified Communications Manager tries to establish a data call with Cisco Jabber by sending an INVITE message to Cisco TelePresence Video Communication Server (VCS). The call is established regardless of receiving a response from VCS.

Client Matter Codes and Force Authorization Codes Not Supported on Cisco Jabber

This documentation update resolves CSCva32400.

The “Client Matter Codes and Forced Authorization Codes” chapter mentions "Mobile phones with Cisco Jabber installed that support CMCs and FACs" as a prerequisite. This information is inaccurate.

Cisco Jabber does not support CMCs or FACs.

Client Matter Codes, Forced Authorization Codes, and Failover Calls

This documentation update resolves CSCuv41976.

The following information is omitted from the “Interactions and Restrictions” section of the Client Matter Codes (CMC) and Forced Authorization Codes (FAC) chapter:

CMCs and FACs do not support failover calls.

Corrected License Report Update Interval

This documentation update resolves CSCuv84693.

The “License Usage Report” topic in the “Licensing” chapter states that “Usage information is updated once daily”. This statement is incorrect.

The correct update interval for the license report (accessed through **System** > **Licensing** > **License Usage Report**) is once every six hours.

Force Authorization Codes Not Supported on Cisco Jabber

This documentation update resolves CSCuz63406.

The “Client Matter Codes and Forced Authorization Codes” chapter states that "Mobile phones with Cisco Jabber installed support CMC and FAC." This information is inaccurate. The correct information is as follows:

Mobile phones with Cisco Jabber installed support only CMC. FACs are not supported.

Gateway Recording Support

The System Requirements topic in the Monitoring and Recording chapter of the *Cisco Unified Communications Manager Features and Services Guide* contains a list of supported gateways for recording, including the ISR-G2 Gateways (29XX, 39XX) running release 15.3(3)M. It should say that release 15.3(3)M or later are supported.

Incorrect Report for Device Mobility

This documentation update resolves CSCuv20382.

The “Device Mobility” chapter incorrectly states to run a report in Cisco Unified Reporting to determine device support for device mobility. Because this feature is related to Unified Communications Manager and not devices, the report does not apply to device mobility.

In Cisco Unified Reporting, “Mobility” refers to WiFi connections.

Jabber Devices Count as Registered Devices

This documentation update resolves CSCur73944.

The following information is omitted from the Limitations section of the “Cisco Unified Mobility” chapter in the *Features and Services Guide*.

When initially configured, Jabber devices count as registered devices. These devices increase the count of registered devices in a node, set by the **Maximum Number of Registered Devices** service parameter.

MGCP FXS Ports Do Not Require a License

This documentation update resolves CSCum47807.

The following note is missing from “Licensing” chapter in the *Features and Services Guide*:

Note MGCP FXS ports do not require any license because they are not considered to be analog phones.

Music On Hold and Native Call Queuing Behavior

The *Announcements with Music On Hold* document discusses Native Call Queuing and the added capabilities that are related to customized audio announcements and Music On Hold. Access this document at the following URL:

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-technical-reference-list.html

Remote Destination and Auto Answer

This documentation update resolves CSCtd43582.

The following restriction is omitted from the "Cisco Mobility" chapter in the *Features and Services Guide for Cisco Unified Communicatins Manager*:

A remote destination call does not work when Auto Answer is enabled.

Restart Intercluster Lookup Service

This documentation update resolves CSCuv11445.

The following information is omitted from "ILS Troubleshooting Tips" in the "Intercluster Lookup Service" chapter of the *Features and Services Guide*:

If you receive an error message when trying to establish ILS between your clusters, you can try to restart the Cisco Intercluster Lookup service from Cisco Unified Serviceability Administration.

SAML SSO Authentication LDAP Attribute for User ID Setting

This documentation update resolves CSCuq44567.

The following note is missing from the "SAML Single Sign-On" chapter in *Feature and Services Guide for Cisco Unified Communications Manager*.

Note Cisco Unified Communications Manager currently supports only sAMAccountName option as the LDAP attribute for user ID settings.

Video Capabilities and Enhanced Location Call Admission Control

This documentation update resolves CSCut20187.

The following information is omitted from the Limitations section in the "Enhanced Location Call Admission Control" chapter:

If video capabilities are enabled, then bandwidth for audio will be allocated from video.

Phone Displaying To Conference

This documentation update resolves CSCus42103.

Procedure

Step 1 Configure a Call Manager cluster with 1 Publisher (CmA11) and 1 Subscriber (CmA2).

Step 2 Phones A, B, C are registered with CmA1 and phone D is registered with CmA2.

Step 3 Setup a consultative or blind ad-hoc conference between A(1000), B(4000), C(5000) and D(6000) with A as the controller.

Step 4 Shutdown CmA2.
Phone D will go to Preservation mode. Phone A,B & C are switched to conference mode.

Step 5 Disconnect Phone A . Phone B & C should be in a Direct call.
Issue: Phone B & C are still in conference.

Step 6 Disconnect Phone B. There should be no call on phone C.
Issue: Phone C is still in Conference.

Call Pickup Restriction

This documentation update resolves CSCuy92491.

The following restriction is omitted from the "Call Pickup" chapter in the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Restriction	Description
Incoming Calling Party International Number Prefix - Phone	If you have configured a prefix in the “Incoming Calling Party International Number Prefix - Phone ” service parameter, and an international call is placed to a member in the Call Pickup Group, the prefix does not get invoked in the calling party field if the call gets picked up by another member of the Call Pickup Group.

Installing Cisco Unified Communications Manager

Installation Warnings

This information applies to CSCug48896.

The following information applies when you install an IM and Presence Service cluster:

Warning Do not add a node in the Cisco Unified Communications Manager server list during the installation process.

Warning Complete the installation of the IM and Presence Service database publisher node and confirm that services are running before you begin to install IM and Presence Service subscriber nodes.

JTAPI Developers Guide

MeetMe: Unsupported JTAPI Feature

This documentation update resolves CSCum39340.

Applications that use JTAPI, including Unified Contact Center Express (UCCX), are unable to dial MeetMe conference numbers to begin a MeetMe conference or join an already started MeetMe conference. MeetMe is not a feature supported by JTAPI and therefor any application that uses JTAPI for call control is unable to perform actions on MeetMe conferences. For Unified Contact Center Express (UCCX), this prevents MeetMe conferences DN from being the destination of Place Call script steps.

Managed Services Guide

SNMP Limits

This documentation update resolves CSCuv32781.

The following information is omitted from the "Simple Management Network Protocol" chapter in the *Managed Services Guide*:

Your system does not allow more than ten concurrent polling queries. We recommend a maximum of eight trap destinations; anything higher will affect CPU performance. This requirement applies to all installations regardless of the OVA template that you use.

Unified Communications Manager Alarms

The *Cisco Unified Communications Manager Managed Service Guide* contains a list of system error alarm messages that may not be up to date.

For a complete list of system error messages, see the *System Error Messages* document for your release at the following URL:

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-system-message-guides-list.html

Online Help for Cisco Unified Communications Manager

Backup Device Limit Incorrect in Disaster Recovery System Online Help

This documentation update resolves CSCuu94393.

The Disaster Recovery System online help incorrectly states that you can configure up to fourteen backup devices. The correct limit is ten devices.

Incorrect Description for Destination Number

This documentation update resolves CSCux74230.

The **Remote Destination Configuration Settings** field description in the Cisco Unified CM Administration Online Help incorrectly states that you can "Enter the telephone number for the destination". The correct statement is "Enter the PSTN telephone number for the destination".

Directory Number Field Description Updated

This documentation update resolves CSCuy28500.

The following note is omitted from the "Directory Number Settings" topic in the online help and "User Device Profile Fields Descriptions in BAT Spreadsheet" topic in the *Cisco Unified Communications Manager Bulk Administration Guide*:

Note The "Disable " or "Flash only" setting options apply only for the handset. The led light on the phone button line will still flash.

Remote Destination Configuration Page In the OLH Needs To Be Updated

This documentation update resolves CSCvb88447.

The "Device Menu" chapter in Cisco Unified CM Administration Online Help contains incorrect information in the "Remote Destination Configuration Settings" help page. The following information was either incorrect or omitted in the relevant fields.

- The **Timer Information** field has incorrect information in the help page. It states the time in "milliseconds", the correct time is set in "seconds".
- The **Timer Information**section lists incorrect order in the help page. The correct orders of the fields are: **Delay Before Ringing Timer**, **Answer Too Soon Timer**, and **Answer Too Late Timer**.
- The **Owner User ID** field is omitted. Following is the description for this field:
    - **Owner User ID—** From drop-down list, choose the appropriate end user profile to which the remote destination profile can be associated later.

OS Administration Guide

Time Is Not Manually Configurable

This information relates to CSCul67741.

The following note appears in the Cisco Unified OS Administration user interface in the **Settings** > **Time** menu and the *Cisco Unified OS Administration Guide*:

Note Before you can manually configure the server time, you must delete any NTP servers that you have configured.

Because it is mandatory to have at least one NTP server, this note is inaccurate. The following is the correct note:

Note You cannot configure time manually from the **Time** window, because you cannot delete all NTP servers and one NTP server is required.

Add CA Signed CAPF Root Certificate to Trust Store

This documentation update resolves CSCut87382.

The following procedure is omitted from the “Manage Certificates” section in the “Security” chapter.:

When using a CA signed CAPF Certificate, follow these steps to add the root certificate to the CallManager trust store.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/Certificate chain**.

Step 3 In the **Upload Certificate/Certificate chain** popup window, select **CallManager-trust** from the **Certificate Purpose** drop-down list and browse to the CA signed CAPF root certificate.

Step 4 After the certificate appears in the **Upload File** field, click **Upload**.

Real-Time Monitoring Tool Guide

Analyze Call Path Tool does not Work with Non-English Language

This documentation update resolves CSCuq28511.

The following note is omitted from the "Cisco Unified Analysis Management" chapter in the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Caution The Analyze Call Path Tool might not work correctly if your computer is set to a language other than English.

Incorrect Default Value for LogPartitionLowWaterMarkExceeded Alert

This documentation update resolves CSCuq39087.

The default threshold value for LogPartitionLowWaterMarkExceeded alert is incorrectly described in the *Cisco Unified Real-Time Monitoring Tool Administration Guide*. The following table contains the correct value.

Table 4: Default Configuration for the LogPartitionLowWaterMarkExceeded RTMT Alert

Value	Default Configuration
Threshold	Trigger alert when following condition met: Log Partition Used Disk Space Exceeds Low Water Mark (90%)

Incorrect Minimum Rate for Monitoring a Performance Counter

This documentation update resolves CSCuz11160.

The *Real-Time Monitoring Tool Guide* states an incorrect minimum amount for monitoring a performance counter. This is the correct statement:

High-frequency polling rate affects the performance on the server. The minimum polling rate for monitoring a performance counter in chart view is 5 seconds; the minimum rate for monitoring a performance counter in table view is 5 seconds. The default for both specifies 10 seconds.

LowAvailableVirtualMemory Threshold Value is Incorrect

This documentation update resolves CSCuu72197.

The LowAvailableVirtualMemory threshold value in the *Cisco Unified Real-Time Monitoring Tool Administration Guide* is incorrectly listed as below 30%. The correct value is below 25%.

Security Guide

BAT User Template Accepts Only Hexadecimal Characters

This documentation update resolves CSCul78860.

The table in the "End user digest credential settings" subsection of the "Digest authentication for SIP phones setup" section states that Digest Credentials accepts alphanumeric characters, which is wrong. The Digest Credentials accepts only hexadecimal characters for BAT User Template.

IP Phone SSL VPN not Supported on Third Party Firewalls

This information applies to CSCun49156.

For IP Phones that use SSL VPN, third-party firewalls are not supported.

MGCP FXS Ports Do Not Require a License

This documentation update resolves CSCum47807.

The following note is missing from "Licensing" chapter in the *Features and Services Guide*:

Note MGCP FXS ports do not require any license because they are not considered to be analog phones.

Replace ASA Certificate on AnyConnect VPN Phone

Note When you upload an updated certificate with the same Common Name (CN) to Phone-VPN-trust, you overwrite the old certificate. Upload the new certificate to the subscriber instead of the publisher. Phone-VPN-trust does not replicate to other servers but this process will still add the new certificate to the database for the Phone VPN Gateway configuration. Therefore, the old certificate will not be overwritten.

Procedure

Step 1 Install the new ASA certificate on the ASA, but do not activate it.

Step 2 Add the new ASA certificate to the trust store (Phone-VPN-trust).

Step 3 Add the new ASA certificate to VPN Gateway Configuration. Select and add the new ASA certificate to "VPN certificates in this location."

Step 4 Gather information about which VPN phones are registering and which VPN phones are not registering.

Step 5 Apply the new configuration file to the phones from the **Common Phone Profile Configuration** window that is used for VPN phones or from the **Device Pool Configuration** window that used for VPN phones.

Step 6 Reset the VPN phones.

Step 7 Ensure that the phone received the updated configuration file or verify that the phone has the new ASA certificate hash information in its configuration file.
For more information, see https://supportforums.cisco.com/document/33891/ip-phone-ssl-vpn-asa-using-anyconnect.

Step 8 Activate the new ASA certificate on the ASA.

Step 9 Verify that the previously registered VPN phones are registering back to Unified Communications Manager.

Step 10 Repeat Steps 4, 5, 6, and 8.

Step 11 Remove the old ASA certificate from the VPN Gateway Configuration.

Secure and Nonsecure Indication Tone

This documentation update resolves CSCuq04604.

In the *Cisco Unified Communications Manager Security Guide*, the section about secure and nonsecure indication tones states that "Protected devices can call nonprotected devices that are either encrypted or nonencrypted. In such cases, the call specifies nonprotected and the nonsecure indication tone plays." This statement applies only if a protected phone calls a nonencrypted, nonprotected phone. If the call is encrypted for both parties, the indication tone plays the secure tone.

Protected devices that call nonprotected devices that are encrypted play the secure tone, while protected devices that call nonprotected and nonencrypted devices play the nonsecure tone.

CSCup54818 Support for CA Certificates in Mixed Mode

If you run your system in mixed mode, some endpoints may not accept CA certificates with a key size of 4096 or longer. To use CA certificates in mixed mode, choose one of the following options:

- use certificates with a certificate key size less than 4096
- use self-signed certificates

Enable Password Persistence

This documentation update resolves CSCuy05368.

The following information is omitted from the "Configure VPN Feature Parameters" section of the VPN Feature Setup chapter in the *Cisco Unified Communications Manager Security Guide*:

When True, a user password gets saved in the phone, if Reset button or "**#**" is used for reset. The password does not get saved and the phone prompts for credentials if the phone loses power or you initiate a factory reset.

Default: False

Resync Bandwidth Option is Removed

This documentation update resolves CSCuz42447. The **Call Admission Control** chapter in *Cisco Unified Communications Manager System Guide* contains incorrect information about the Bandwidth Calculations field. This option of resync bandwidth is no longer required and the following has been omitted from the guide:

When a link to a location experiences blockage, it may result from bandwidth leakage that has reduced the usable bandwidth for the location. You can resynchronize the bandwidth allotment to the maximum setting for the location without restarting the Cisco Unified Communications Manager server. If you resynchronize the bandwidth for a location when calls are using the link, the bandwidth might be oversubscribed until all calls that are using the link disconnect. An oversubscribed link can cause audio and video quality to degrade. For this reason, resynchronize the location bandwidth during hours when the link has low traffic.

CNF File Encryption Is Not Supported by Default on 6901 and 6911, Cisco IP Phones

This documentation update resolves CSCuz68165.

The following note is omitted from the "Phone Models Supporting Encrypted Configuration File" topic in the *Security Guide for Cisco Unified Communications Manager*.

Note Cisco Unified IP Phones 6901 and 6911 do not request for the ITL file as they do not support security by default. Therefore, the Cisco Unified Communications Manager cluster should be set to secure (Mixed) mode for the Cisco Unified IP Phones(6901 and 6911) to get the Cisco CTL file containing Cisco Certificate Authority Proxy Function (CAPF) details for the encrypted configuration file to work on the Cisco IP Phones (6901 and 6911).

ITL File Size Limitation

This documentation update resolves CSCvb44649.

The following information is omitted from the "Initial Trust List " chapter of the *Security Guide for Cisco Unified Communications Manager*:

If a Cisco Unified Communications Manager cluster has more than 39 certificates, then the ITL file size on Cisco Unified IP Phone exceeds 64 kilobytes. Increase in the ITL file size affects the ITL to load properly on the phone causing the phone registration to fail with Cisco Unified Communications Manager.

Serviceability Guide

AXL Web Service Requirement for ICSA HA

This documentation update resolves CSCup00956.

Information regarding the Cisco AXL Web Service for interclustering on IM and Presence Service was updated as follows:

- Turn on this service on the first node only if there is no intercluster communication configured.
- If intercluster communication is configured, this service must be enabled on both nodes in the sub-cluster where remote peers are configured to sync from.
- Failure to turn on this service causes the inability to update IM and Presence from client-based applications that use AXL.

Cisco CAR DB Service

This documentation update resolves CSCup98304.

The following service is omitted from the "Services" chapter in the *Cisco Unified Communications Manager Serviceability Guide* and online help.

Cisco CAR DB Service

Cisco CAR DB manages the Informix instance for the CAR database, which allows Service Manager to start or stop this service and to bring up or shut down the CAR IDS instance respectively. This is similar to the Unified Communications Manager database that is used to maintain the CCM IDS instance.

The Cisco CAR DB service is activated on the publisher by default. The CAR DB instances are installed and actively run on the publisher, to maintain the CAR database. This network service is used only on the publisher and is not available on the subscribers.

Cisco Certificate Change Notification Service

This documentation update resolves CSCup84785.

The following content is omitted from the Platform Services section of the "Services" chapter in the *Cisco Unified Serviceability Administration Guide:*

Cisco Certificate Change Notification Service

This service keeps certificates of components like Tomcat, CallManager, and XMPP automatically synchronized across all nodes in the cluster. When the service is stopped and you regenerate certificates, you have manually upload them to Certificate Trust on the other nodes.

Cisco IP Phone Service Removed from CM Services

This documentation update resolves CSCur03499.

The Service groups and CM Services sections in *Cisco Unified Serviceability Administration Guide* mention Cisco IP Phone Service. This service has been removed from CM Services as IP Phone services is offered through the User Data Services (UDS) component starting Cisco Unified Communications Manager, Release 10.0(1).

Cisco SOAP-CallRecord Service

This documentation update resolves CSCup98302.

The following service is omitted from the "Services" chapter in the *Cisco Unified Communications Manager Serviceability Guide* and online help.

Cisco SOAP-CallRecord Service

The Cisco SOAP-CallRecord service runs by default on the publisher as a SOAP server, so that the client can connect to CAR database through the SOAP API. This connection happens through the use of the CAR connector (with a separate CAR IDS instance).

SNMP Limits

This documentation update resolves CSCuv32781.

The following information is omitted from the "Set up SNMP" procedure in the "Simple Management Network Protocol" chapter in the *Serviceability Administration Guide*:

Your system does not allow more than ten concurrent polling queries. We recommend a maximum of eight trap destinations; anything higher will affect CPU performance. This requirement applies to all installations regardless of the OVA template that you use.

IM and Presence Security Best Practice

This documentation update resolves CSCuz69271. The following note is omitted from the "Services" chapter in **Cisco Unified Serviceability Administration Guide**.

Devices using IM and Presence are configured to use a Postgres external database to support persistent chat, compliance, and file transfer. However, the connection between IM and Presence server and Postgres is not secured and the data passes without any check. For the services or devices that do not support TLS, there is another way to provide secure communication by configuring IP Sec, which is a standard protocol for secure communications by authenticating and encrypting each IP packet of a communication session.

SOAP-Diagnostic Portal Database Service

This documentation update resolves CSCuq22399.

The following service is omitted from the "Services" chapter in the *Cisco Unified Communications Manager Serviceability Guide* and online help.

SOAP-Diagnostic Portal Database Service

The Cisco Unified Real-Time Monitoring Tool (RTMT) uses the SOAP-Diagnostic Portal Database Service to access the RTMT Analysis Manager hosting database. RTMT gathers call records based on operator-defined filter selections. If this service is stopped, RTMT cannot collect the call records from the database.

Error in SYSLOG-MIB Parameters

This documentation update resolves CSCux59529.

The "CISCO-SYSLOG-MIB Trap Parameters" topic incorrectly lists the command for "Set clogMaxSeverity" as **snmpset -c public -v2c 1<transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>**.

The correct command is **snmpset -c public -v2c <transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>**.

System Guide

Call Transfer to Hunt Pilot Restriction

This documentation update resolves CSCuw57732.

The following information is omitted from the "Phone Features" section in "Cisco Unified IP phones" chapter:

If a call transfer to a hunt pilot is initiated when an announcement is in progress, the call is redirected only after the announcement is complete.

Email IDs on the Active Directory Server

This documentation update resolves CSCur55902.

The following information is omitted from the "Directory Overview" in the *Cisco Unified Communications Manager System Guide*.

Note For the users that must be synchronized to the Cisco Unified Communications Manager database, their email ID fields on the active directory server must be unique or blank.

LDAP Directory Support

The "Configure LDAP Directory" topic in the *Cisco Unified Communications Manager System Guide, Release 10.0(1)* contains a list of supported LDAP directories. However, this list should include Microsoft Active Directory 2012 and Microsoft Lightweight Directory Services 2012 R1/R2.

The complete list of supported directories is as follows:

- Microsoft Active Directory 2003 R1/R2
- Microsoft Active Directory Application Mode (ADAM) 2003 R1/R2
- Microsoft Active Directory 2008 R1/R2
- Microsoft Lightweight Directory Services 2008 R1/R2
- Microsoft Active Directory 2012 R1/R2
- Microsoft Lightweight Directory Services 2012 R1/R2
- Sun One 6.x
- Sun Directory Services 7.0
- Oracle Directory Services Enterprise Edition 11gR1 (v11.1.1.5.0)
- OpenLDAP 2.3.39 & 2.4.x

Bandwidth Calculations

This documentation update resolves CSCuz42436. The **Call Admission Control** chapter in *Cisco Unified Communications Manager System Guide* contains incorrect information about the Bandwidth Calculations field. It is mentioned that the iLBC call uses 24 kb/s. The correct bandwidth consumption at 20ms should be 31.2kb/s.

Insufficient Information About Third-Party Restrictions

This documentation update resolves CSCvc16660.

The following restriction is omitted from the "Configure Third-Party SIP Phones" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*:

Restriction	Description
Ringback tone restriction for Cisco Video Communications Server (VCS) registered to third-party SIP Endpoints	Blind transfer or switch to request the transfer which occurs over VCS registered endpoints with Cisco Unified Communications Manager will not have a ringback tone. If you do a supervised transfer, then you allocate Music On Hold (MOH) but, not a ringback tone.

Time of Day routing not Implemented for Message Waiting Indicator

This documentation update resolves CSCva13963.

The following information is omitted from the "Configure Time of Day Routing" topic in the *System Configuration Guide for Cisco Unified Communications Manager*.

Time of Day routing is not implemented for Message Waiting Indicator intercept.

TCP and UDP Port Usage Guide

Intercluster Lookup Service Name Correction

This documentation update resolves CSCuy48640.

The “Common Service Ports” table incorrectly describes ILS as Intracluster Lookup Service. The following table contains the correct name.

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager	Unified Communications Manager	7501	Used by Intercluster Lookup Service (ILS) for certificate based authentication.

Missing Information about TCP Port 22

This documentation update resolves CSCus05634.

The following entry is omitted from the “Intracluster Ports Between Cisco Unified Communications Manager Servers” table in the *TCP and UDP Port Usage Guide for Cisco Unified Communications Manager* :

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager Publisher	Unified Communications Manager Subscriber	22 / TCP	Cisco SFTP service. You must open this port when installing a new subscriber.

Missing Information about TCP Port 5555

This documentation update resolves CSCus26925.

The following entry is omitted from the “ Web Requests From CCMAdmin or CCMUser to Cisco Unified Communications Manager” table in the *TCP and UDP Port Usage Guide for Cisco Unified Communications Manager* :

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager	Cisco License Manager	5555 / TCP	Cisco License Manager listens for license requests on this port

Missing Information about Common Service Port 8006

This documentation update resolves CSCuy48628.

The following entry is omitted from the " Common Service Ports " table in the *TCP and UDP Port Usage Guide for Cisco Unified Communications Manager* :

From (Sender)	To (Listener)	Destination Port	Purpose
ILS Service Port		8006 / TCP	

Upgrade Guide

Disable or Postpone LDAP Synchronization During an Upgrade

This document update resolves CSCuq07331.

The following information is omitted from the "Preupgrade Tasks" chapter in the *Upgrade Guide for*

It is recommended that you disable or postpone the LDAP synchronization on Unified Communications Manager during an upgrade. If the synchronization is scheduled in for a time period which falls after the Unified Communications Manager upgrade and before the IM and Presence Service upgrade, then the result can negatively affect the IM and Presence Service if user changes occurred in this timeframe.

Unified CM 10.0 Upgrade Process Correction

This documentation update resolves CSCup31306.

In the Change Virtual Machine Configuration Specifications procedure, Step 6 ("Shut down the virtual machine") should be performed before Step 3 ("Change the configuration of the virtual machine").

InterCluster Peer-User and Admin-CUMA Application User Roles Deprecated

The application user group roles InterCluster Peer-User and Admin-CUMA are deprecated from release 10.0(1). Any application users with these roles configured in releases 8.x or 9.x have the roles removed during an upgrade to any 10.x release. After the upgrade the administrator must configure appropriate roles for these users.

Note For intercluster to function correctly, the AXL user defined on the IM and Presence Service user interface (**Presence** > **Inter-Clustering**) must have a Standard AXL API Access role associated with it on the Cisco Unified Communications Manager application user page.

Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service

Domain Name Change for Cisco Unified Communications Manager

This documentation update resolves CSCuw76028.

The following information is omitted from the " Domain Name and Node Name Changes" chapter in the *Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service Guide*.

Update Domain Name for Cisco Unified Communications Manager

You can use the Command Line Interface (CLI) to change the domain name for Cisco Unified Communications Manager. Update the DNS domain name on all applicable nodes using the CLI. The CLI command makes the required domain name change on the node and triggers an automatic reboot for each node.

Before You Begin

- Perform all pre-change tasks and the applicable system health checks.
- Ensure to enable the DNS before changing the domain name.
- If the server table has an existing hostname entry, first change the hostname entry of the domain name.

Procedure

Step 1 Log in to Command Line Interface.

Step 2 Enter **run set network domain <new_domain_name>**
The command prompts for a system reboot.

Step 3 Click **Yes** to reboot the system.
The new domain name gets updated after the system is rebooted

Step 4 Enter the command **show network eth0** to check if the new domain name is updated after the reboot.

Step 5 Repeat this procedure for all cluster nodes.

What to Do Next

For more information, see the " Post-Change Tasks and Verification" chapter in the *Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service guide*.

Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager

Retrieve Chat Rooms on a Replaced Node

This documentation update resolves CSCuy96037.

The following information is omitted from the “Chat Node Alias Management” topic in the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* guide.

To ensure that the user has access to all the old chat rooms, take a backup of all the existing aliases before deleting a node and assign the same alias to a new node.