Release Notes for Cisco Unified Communications Manager and IM and Presence Service, Release 9.0(1)

First Published: 2012-07-18

Last Modified: 2013-10-05

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-26027-01

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)

© 2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface xiii

Purpose xiii

Organization xiv

Audience xiv

Conventions xv

Obtain Support xvi

CHAPTER 1

Introduction 1

Hardware server requirements 1

Server software requirements 4

Supported browsers 4

CHAPTER 2

Upgrading to Unified CM Release 9.0(1) 7

Software Version Number 8

Pre-Upgrade Tasks 8

Software Upgrade Considerations 10

Overview of Software Upgrade Process 10

Upgrading on a Virtual Server 10

Configuration Changes During Upgrade 11

Supported Upgrades 11

Upgrade File 12

Upgrade Media 12

Software Upgrade Procedures 12

Install the COP File 12

Upgrade to Restricted or Unrestricted Unified Communications Manager 13

Upgrade From a Local Source 13

Upgrade From a Remote Source 15

Supported SFTP Servers 15
Bridge Upgrade 17
Post-Upgrade Tasks 17
Latest Software and Firmware Upgrades 17
Firmware 17
Software 18
Related Documentation 18
Limitations and Restrictions 18

CHAPTER 3 Upgrading to IM and Presence Release 9.0(1) 21
New system installation information 21
System Upgrade 21
Supported upgrade paths to IM and Presence Release 9.0(1) 21
Upgrade from Cisco.com 22
Upgrade order 23
Software licensing requirements for VMware 23
Recommendations for release 8.0(x), 8.5(x), or 8.6(x) to 9.0(1) upgrades 23

CHAPTER 4 Important Notes 25
Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets 26
Cisco Unified Mobility Disclaimer 26
Configure LDAP Directory 26
DoCoMo Phones Not Certified 27
Install Language Prompts for TAPS 27
IPv4-Only Support for Video Streams 27
Jabber Certificate Warnings with IM and Presence Service 28
LBM Hub Node TCP Port 9004 Must Only Be Accessible by Trusted Nodes 28
Locale Installer Locale File for Belgium 28
Localization Not Supported for Some Unified CM Components 28
RD Numbers Cannot Be Provisioned on Two Different Clusters 29
Unified CM Assigns a Nonsecure Conference Bridge When the Conference is Initiated by a Nonsecure Phone 29
Upgrade Restores Configure Automatic Database Purge Parameter Default 29
Devices Reset while Certificate Regeneration 29

MGCP IOS Gateway From PSTN Does Not Support Connected Address in ISDN Notify 29
Perfect Forward Secrecy is not Supported in IPsec Configuration 30
Change Perfmon Counter File Size Parameters in RTMT 30

CHAPTER 5 New and Changed Information 31
Integration of Unified CM and IM and Presence 31
Deprecated Features 32
Licensing 32

CHAPTER 6 Caveats 35
Bug Fixes and Updates 35
Bug Search Tool 35
Resolved Caveats 36
Open Caveats 36
Open Caveats for Unified CM Release 9.0(1) 37
Open Caveats for IM and Presence Release 9.0(1) 48

CHAPTER 7 Documentation Updates 49
License Mac References 50
Administration Guide 50
Access Control Group Permissions Interactions 50
Application User AXL Password Must Not Contain Special Characters 50
BFCP is Supported with TelePresence MCU 51
Convert LDAP Synchronized User to Local User Check Box Field Description Is Missing 51
Connected Lined ID Presentation Value 51
Call Stats Field Removed 52
Common Phone Profile Settings Secure Shell Information 52
Default Device Pool May Not Be Chosen After Upgrades to 5.x or Later 52
Device Mobility Calling Search Space is Used When Device CSS is set to None 52
End User Settings Correction 52
Hostnames in IPv4 and IPv6 Environments 52
Hub_None Location Correction 53
An ILS Restart is Required for Changes to Directory URI Catalogs 53
Incorrect Information about Deleting Route Patterns 53
Incorrect Note about User Locales 54

Line Group Deletion Correction 54
Link Loss Type Field is Relabeled 54
Maximum Hunt Timer Restriction 54
Missing Exceptions for Voicemail Pilot 55
Missing Tip for Naming a Server 55
Option For Voicemail Usage Description 55
Phone Support for Multilevel Precedence and Preemption 55
Route Class Configuration SIP Information 56
Service Name Cannot Be Localized 56
Service Profiles and Device Owner User IDs 56
Transmit UTF8 for Calling Party Name Field Correction 56
Use Personal Preference Field is Relabeled 57
Directory Number Field Description Updated 57
Correction in Software Conference Bridge Maximum Audio Streams 57
Bulk Administration Guide 57
Cannot Disassociate Devices from End Users Using BAT 57
FindAndList Gateway Template Does Not Display the Templates 58
Missing Note in Insert Phone Topic 58
Model Is Not a Valid Device Field When Generating Phone Reports 58
Call Detail Records Administration Guide 58
Call Recording Samples in CDR Examples Chapter 58
Change Order of HuntPilotDN 60
FinalCalledPartyNumber Field Description Is Incorrect 60
Missing CDR Field Descriptions 60
Missing CDR Field Descriptions for IMS Application Server 61
FAC and CMC Code is not Captured in CDR 62
Changing IP Address and Hostname 65
Change the Hostname Using the Unified Communications Operation System Administration GUI 65
Missing Step in Unified CM Hostname Update 65
Command Line Interface Reference Guide 66
ILS Troubleshooting Tips Corrections 66
Show perf query counter Command Output 67
Trace Option for Show Media Streams CLI Command 67
Deployment Guide for IM and Presence Service 67

Exceeding Maximum Contact List Settings During Contact List Import Is Supported 67
Legacy Clients 67
Dialed Number Analyzer Guide 68
Find and List Phones in DNA Using Directory URI 68
Disaster Recovery System Guide 68
Supported SFTP Servers 68
System Backup File Encryption 69
Updated Caution to Include DNS and Domain Name Prior To Restore 69
Features and Services Guide 69
Answer Too Late Timer 69
Call Mobility Missing Information 70
Call Park Display Timer Restriction 70
Call Pickup Phones Supported 70
Call Queuing Interaction with Hunt Groups and Hunt Pilots 70
Call Queuing Missing Information 71
Call Queuing Not Supported with Mobile Device Types 71
Call Queuing Shared Line Scenario Description 71
Call Waiting Behavior with MLPP Preemption Correction 71
Calling Party Normalization Restriction 71
Centralized Proxy TFTP File Signature Verification Failure 72
Cisco Unified Communications Manager Sends INVITE Message to VCS 72
Client Matter Codes, Forced Authorization Codes, and Failover Calls 72
Configuring OpenAM Section 72
Corrected License Report Update Interval 73
Corrections for the Immediate Divert Feature 74
Early Media Cut-Through and Single Number Reach Missing Information 75
EMCC Logout Limitation 75
EMCC Remote Cluster Menu 75
Empty Far-End When Recording Call Park for Some Phones 75
Enable Mobile Connect for IP Multimedia Subsystem 75
Enterprise Feature Access and User Control 76
Expansion Module Field Missing From Certain Device Profiles 76
Extension Mobility Equivalency Changes 76
Extension Mobility Missing Information 77
Hunt Pilots Limit for a Call Queue 78

iDivert Feature Correction 78
Incorrect Report for Device Mobility 78
MGCP FXS Ports Do Not Require a License 79
MLPP Parameters 79
New Audio Files for Music On Hold 79
No Audio After Pressing Mobility Button 80
Play Continuously and Music On Hold 80
Queue Status PLK Supported Phone Models 80
Remote Destination and Auto Answer 80
Remote Destination Single Number Reach and Enterprise Number Call Reroute 81
Restart Intercluster Lookup Service 81
Secure Shell Password Maximum Length 81
SIP Phones Support CMC and FAC Tones 81
Support for Midcall Mobility Features with Cisco Unified Border Element 82
User Control System Parameters Correction 82
Call Pickup Restriction 82
4000 Series Integrated Services Routers do not support Mobile Voice Access 82
Installing Cisco Unified Communications Manager 83
Cisco Unified CM Installation on MCS 7825 H3 and 7828 H3 Server Models 83
Disable ICH10 Onboard SATA Controller on EX/ESXi Servers During Unified CM Installation 84
Installation Fails with Unrecoverable Internal Error 84
Post-Installation Tasks 85
Interdomain Federation for IM and Presence Service 85
Cannot Install Signed Microsoft CA Server-Client Authentication Certificate on Microsoft OCS 2008 85
FIPS Not a Requirement for Federated Connections with LYNC 2010 Servers 86
Use TLS for Static Routes 86
Managed Services Guide 86
SNMP Limits 86
Unified Communications Manager Alarms 87
Online Help 87
OS Administration Guide 89
ICSA Service Needs Restart After Ipsec Cert Is Regenerated 89
Regenerate Certificate 89

Partitioned Intradomain Federation for IM and Presence Service 91
Disable Empty TLS Fragments 91
FIPS Not a Requirement for Federated Connections with LYNC 2010 Servers 91
MatchUri Set to IM and Presence Service Domain 91
Use TLS for Static Routes 91
Real-Time Monitoring Tool Guide 91
Alert Removal 91
CallProcessingNodeCpuPegging Alerts for VMware Installations 92
Incorrect Default Value for LogPartitionLowWaterMarkExceeded Alert 92
LowAvailableVirtualMemory Threshold Value is Incorrect 92
Missing Content from Mailbox Sync Counters 93
RTMT Cannot Collect OPC Logs Under Default Settings 94
Security Guide 94
BAT User Template Only Accepts Hexadecimal Characters for Digest Credentials 94
Bulk Certificate Import May Cause Phones To Restart 94
CTL File Size Limit Correction 95
Encryption Protocols Specifications Missing for Phone Models 95
Refresh Upgrade Update 96
Secure Call Monitoring and Recording Update 96
SSL and TLS Support 96
Updated Note for Rollback Cluster to Pre-8.0 97
Incorrect Configuration Example for ASA Router 97
CNF File Encryption Is Not Supported by Default on 6901 and 6911, Cisco IP Phones 99
ITL File Size Limitation 99
Serviceability Guide 100
Audit Log Configuration Settings 100
Audit Log Severity Levels 100
AXL Web Service Requirement for ICSA HA 100
Cisco CAR DB Service 101
CAR Database Update 101
Cisco Certificate Change Notification Service 101
Cisco SOAP-CallRecord Service 101
SNMP Limits 102
IM and Presence Security Best Practice 102
SOAP-Diagnostic Portal Database Service 102

User Options Logging 102
Platform Administrative Web Service 103
SIP Transparency and Normalization Developers Guide 103
Cause Tag Required for convertHIToDiversion() API 103
System Guide 103
Bandwidth Management Sections of Video Telephony in the 9.x System Guide 103
Call Preservation Support for SIP Trunks 104
Insufficient Information About Third-Party Restrictions 104
LDAP Synchronized and Local End Users 104
Phones that Support International Escape Character 104
Presentation Sharing Supported with BFCP 105
SCCP Device Handles One Call in a Pending State 105
SIP Redirect by Application Requires a SIP Route Pattern 105
Transcoding G.711 to All Codecs Supported 106
Trunk Types 106
Video Resolution Support for SIP Phones 106
Time of Day routing not Implemented for Message Waiting Indicator 107
TCP and UDP Port Usage Guide 107
Port Information for UDS 107
Missing Information about TCP Port 22 107
Missing Information about TCP Port 5555 107
Missing Information about Common Service Port 8006 108
Upgrade Guide 108
Adding a New Subscriber Causes Device Reset 108
Downtime When Upgrading Publisher Server Until All Subscriber Servers Are Updated 108
Preupgrade Step to Check Connectivity 108
Presence Data Loss After Upgrade From Cisco Business Edition 5000 to Cisco Unified Communications Manager 109
Presence User Experiences Issues Obtaining Availability 109
User Options Guide 109
The Fast Dial User Option is Not Supported 109
XML Developers Guide 110
MaxReturnedDevices in Serviceability XML 110
Serviceability XML API Doc in Error 110

Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service 110
Domain Name Change for Cisco Unified Communications Manager 110
Update Domain Name for Cisco Unified Communications Manager 110
Online Help for Cisco Unified Communications Manager 111
Incorrect Description for Destination Number 111
Directory Number Field Description Updated 111
Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager 112
Retrieve Chat Rooms on a Replaced Node 112

Preface

Release notes for previous versions of the following products are available:

- Cisco Unified Communications Manager-http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html
- Cisco Unified Communications Manager Business Edition 5000-http://www.cisco.com/en/US/products/ps7273/prod_release_notes_list.html.
- Cisco Unified Communications Manager IM and Presence Service-http://www.cisco.com/en/US/products/ps6837/prod_release_notes_list.html

Note Beginning with Release 9.0(1), Cisco Unified Presence has been rebranded to IM and Presence Service, however, the IM and Presence Service continues to run on its own MCS hardware or virtual machine instance.

Before you install or upgrade Cisco Unified Communications Manager (Unified Communications Manager) or the IM and Presence Service, Cisco highly recommends that you review the following sections of this document:

- Purpose, page xiii
- Organization, page xiv
- Audience, page xiv
- Conventions, page xv
- Obtain Support, page xvi

Purpose

This document provides information about the latest release of Cisco Unified Communications Manager and IM and Presence.

Organization

The following table shows how this guide is organized:

Table 1: Updates to Release Notes for Cisco Unified Communications Manager

Chapter	Description
Introduction	This chapter provides a brief description of Unified Communications Manager and IM and Presence as well as the system requirements for both products.
Upgrading to Unified Communications Manager	This chapter provides critical information about upgrading to this release of Unified Communications Manager.
Upgrading to IM and Presence	This chapter provides critical information about upgrading to this release of IM and Presence.
Important Notes	This chapter highlights important notes to consider in this release of Unified Communications Manager and IM and Presence.
New and Changed Information	This chapter lists and describes new features and changes to existing behavior for both Unified Communications Manager and IM and Presence.
Caveats	This chapter provides a snapshot of open caveats for both Unified Communications Manager and IM and Presence.
Documentation Updates	This chapter provides a description of documentation updates made in this release for both Unified Communications Manager and IM and Presence.

Audience

This document provides information for network administrators who are responsible for managing and supporting Cisco Unified Communications Manager and IM and Presence. Network engineers, system administrators, or telecom engineers use this guide to learn about key features and documentation updates, open caveats, and installation and upgrade considerations in this release.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in screen font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in italic screen font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

Timesaver Means the described action saves time. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

Tip Means the information contains useful tips.

Cautions use the following conventions:

Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

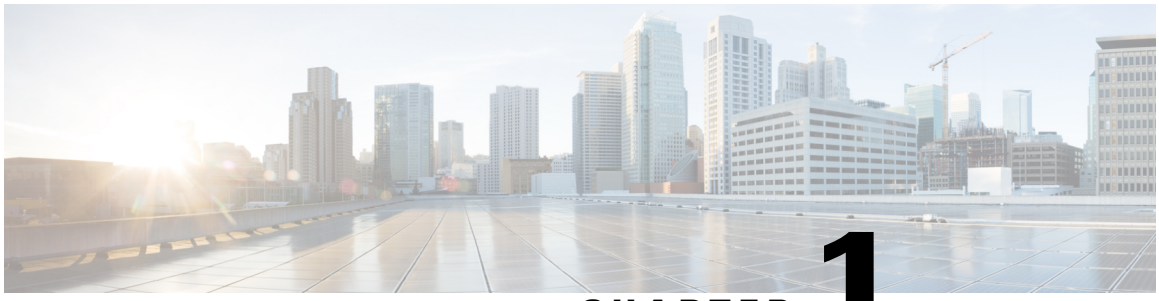
Warnings use the following conventions:

Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.

Obtain Support

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at

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



CHAPTER 1

Introduction

These release notes describe new features, requirements, restrictions, and caveats for both 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, voice-over-IP (VoIP) gateways, mobile devices, and multimedia applications.

The 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 amongst 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 Cisco System's ability to supply Unified Communications Manager and IM and Presence Service worldwide. Cisco has obtained an unrestricted US export classification to address this issue.

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

Before you install or upgrade either product, Cisco recommends that you review the Related Documentation, on page 18 for information about the documentation available.

- Hardware server requirements, page 1
- Server software requirements, page 4
- Supported browsers, page 4

Hardware server requirements

The following sections describe the system requirements for this release of Cisco Unified Communications Manager and IM and Presence.

Server support for Cisco Unified Communications Manager

Make sure that you install and configure Unified CM and IM and Presence on a Cisco Media Convergence Server (MCS), a Cisco Unified Computing System (UCS) server, a Cisco-approved HP server configuration, or a Cisco-approved IBM server configuration. For information about which MCS and UCS servers are compatible with this release of Unified CM or IM and Presence, see the related compatibility matrix.

- *Hardware and Software Compatibility Information for IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1)*-http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html
- *Supported Servers for Releases of Cisco Unified Communications Manager and Cisco Intercompany Media Engine*-http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/prod_brochure0900aecd8062a4f9.html

Server support for the IM and Presence Service

Note The IM and Presence Service requires 4 GB of RAM, except for the 500 user and Business Edition 6000 OVA deployments, which require 2 GB of RAM.

The IM and Presence service is software that is loaded onto a hardware server. The hardware server must meet the following requirements:

- One of the following server models:
  - Cisco 7800 Series Media Convergence Server (MCS) listed in the *Hardware and Software Compatibility Information for IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1)*. Go to Cisco.com for the latest information:

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

    Note IM and Presence does not support MCS-xxxx-I1-IPC1 or MCS-xxxx-H1-IPC1 servers. However, a bridged upgrade is available to customers who need to migrate from any of the discontinued hardware, except for the following servers: MCS-7825-H1-IPC1, MCS-7825-I2-IPC1, MCS-7825-I1-IPC1, MCS-7825-I2-IPC2. For details about the unsupported hardware and the bridged upgrade, see the *Upgrade Guide for Cisco Unified Communications Manager, Release 9.0(1)* here: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html
  - Cisco-approved, customer-provided third-party server that is the exact equivalent of one of the supported Cisco MCS servers. Go to http://www.cisco.com/go/swonly.
  - Cisco Unified Computing System B-series blades or Cisco Unified Computing System C-series rackmount servers. For information about these Cisco Unified Computing System servers, see the *Hardware and Software Compatibility Information for IM and Presence Service on Cisco Unified Communications Manager*.
- DVD-ROM drive
- Keyboard, mouse, and monitor

Note Additional server requirements, such as port and IP address requirements, are described in the *Cisco Unified Communications Manager TCP and UDP Port Usage Guide, Release 9.0(1)* here: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/port/9_0_1/CUCM_BK_T98E8963_00_ .

The IM and Presence installer checks for the presence of the DVD-ROM drive, sufficient hard drive and memory sizes, and sufficient CPU type and speed.

IM and Presence supports bridged upgrades from any of the following servers:

- MCS-7825-H2-IPC1
- MCS-7825-H2-IPC2
- MCS-7835-H1-IPC1
- MCS-7835-I1-IPC1
- MCS-7845-H1-IPC1
- MCS-7845-H2-IPC1 (only if each of the two disks has less than 72GB of storage space, otherwise it is fully supported)
- MCS-7845-I1-IPC1

The bridged upgrade allows you to create a DRS backup on the discontinued hardware. You can then restore the DRS backup on supported hardware after you complete a fresh IM and Presence installation on the supported hardware. If you attempt an upgrade on discontinued hardware, a warning displays on the interface on the interface and on the CLI, informing you that Unified CM or IM and Presence only supports the functionality to create a DRS backup on this server.

Uninterruptible power source

Cisco recommends that you connect each Unified CM or IM and Presence server to an uninterruptible power supply (UPS) to provide backup power and protect your system against a power failure.

Caution When the MCS-781x and MCS-782x servers are not connected to a UPS, they run a higher risk of file corruption during power outages because the cached data is lost during a power outage on these servers with drive write cache enabled (and no battery backup). To prevent file system corruption, you must connect these servers to a UPS.

When Unified CM and IM and Presence run on one of the servers listed in the table below, basic integration to the UPS model APC SmartUPS 1500VA USB and APC 750VA XL USB is supported.

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

Alternatively, you can execute the CLI command **show ups status** to show the current status of the USB-connected APC smart-UPS device and starts the monitoring service if it is not already started. The CLI command also displays detected hardware, detected versions, current power draw, remaining battery runtime, and other relevant status information.

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

For unsupported Unified CM or IM and Presence releases, MCS models or UPS models, you can cause an external scripts to monitor the UPS. When low battery is detected, you can log in to the Unified CM or IM and Presence server by using Secure Shell (SSH), access the CLI, and execute the **utils system shutdown** command.

Note If your pre-9.0 Unified CM or IM and Presence Service runs on a deprecated server, you can upgrade it by using the Bridge upgrade procedure.

Table 2: Supported servers for UPS integration

HP servers	IBM servers	UCS servers
MCS-7816-H3	MCS-7816-I3	B200 M1 Blade Server
MCS-7825-H3	MCS-7816-I4	B200 M2 Blade Server
MCS-7825-H4	MCS-7816-I5	C200 M2 Rack Server
MCS-7828-H3	MCS-7825-I3	C210 M1 Rack Server
MCS-7835-H2	MCS-7825-I4	C210 M2 Rack Server
MCS-7845-H2	MCS-7825-I5	
	MCS-7828-I3	
	MCS-7828-I4	
	MCS-7828-I5	
	MCS-7835-I2	
	MCS-7845-I2	
	MCS-7845-I3	
	MCS-7845-I3	

Server software requirements

Unified Communications Manager and the IM and Presence Service run on the Cisco Linux-based operating system. This operating system is included with the purchase of either application.

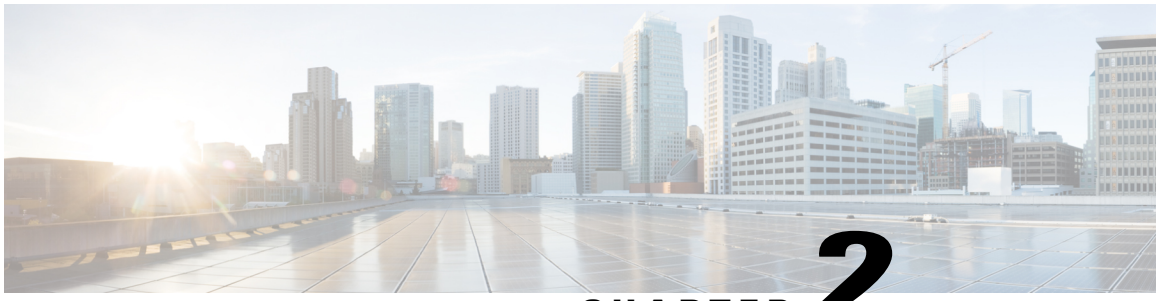
Supported browsers

Use the following Internet browsers to access the Unified Communications Manager and IM and Presence Service interfaces:

- Microsoft Windows: Microsoft Internet Explorer Version 6.0 or later or Mozilla Firefox Version 3.x, 4.x, or 10.x
- Mac: Safari 5.x or Mozilla Firefox Version 4.x or 10.x

The following Internet browsers are officially supported to access the Enterprise License Manager interface:

- Firefox: Version 8, 9, 10
- Internet Explorer: Version 8, 9
- Google Chrome: Version 15, 16, 17
- Safari: Version 5.1



CHAPTER 2

Upgrading to Unified CM Release 9.0(1)

Caution When you upgrade to Cisco Unified Communications Manager 9.0, the system reboots several times as part of the upgrade process and the service outage period is longer than with traditional upgrades. Therefore, you may want to perform the upgrade during a scheduled down time for your organization to avoid service interruptions.

Caution If you upgrade to the U.S. export unrestricted version of Cisco Unified Communications Manager, you will not be able to later upgrade to or be able to perform a fresh install of the U.S. export restricted version of this software. Note that IP phone security configurations will be modified to disable signaling and media encryption (including encryption provided by the VPN phone feature).

Note A non-bootable image is available for download from Cisco.com. This image may be downloaded to a network server (remote source) or burned to DVD (local source) and used for upgrades. DVDs ordered from Cisco are bootable and may be used for fresh installs.

Caution Be sure to back up your system data before starting the software upgrade process. For more information, see the Disaster Recovery System Administration Guide. If you are upgrading your software from a version prior to Release 8.6(x) on HP 7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. If you do not back up your system data before starting the software upgrade process your data will be lost if your upgrade fails for some reason. If you chose to revert to the prior version, you will need to install the prior version and restore your data from your DRS backup.

The following sections contain important information about upgrading to this release of Unified CM:

- Software Version Number, page 8
- Pre-Upgrade Tasks, page 8
- Software Upgrade Considerations, page 10
- Supported Upgrades, page 11

- Upgrade File, page 12
- Upgrade Media, page 12
- Software Upgrade Procedures, page 12
- Post-Upgrade Tasks, page 17
- Latest Software and Firmware Upgrades, page 17
- Related Documentation, page 18
- Limitations and Restrictions, page 18

Software Version Number

These release notes are based on following software version:

- Unified CM: 9.0.1.10000-37

Pre-Upgrade Tasks

You must install all pre-9.0 licenses to Cisco Unified Communications Manager before you upgrade to the latest release. After you upgrade to the latest release, you cannot apply these licenses to Cisco Unified Communications Manager and you cannot apply them using the Enterprise License Manager. Ensure that you install all unused licenses or Product Authorization Keys (PAKs) before you upgrade the system.

To support high availability, Unified Communications Manager Release 9.x clusters operate in a full-featured demo mode for 60 days without a license. After 60 days, the clusters continue to operate and route calls, but the functionality to add or remove devices and users is disabled until valid licenses are available on the associated Enterprise License Manager (ELM).

Before you begin the upgrade, see the following:

- *Upgrade Guide for Cisco Unified Communications Manager*.

Caution When you perform a Refresh Upgrade to the latest release of Cisco Unified Communications Manager, the system reboots several times as part of the upgrade process and the service outage period is longer than with traditional upgrades. Therefore, you may want to perform the upgrade during a scheduled down time for your organization to avoid service interruptions.

Caution If you upgrade to the U.S. export unrestricted version of Cisco Unified Communications Manager, you will not be able to later upgrade to or be able to perform a fresh install of the U.S. export restricted version of this software. Note that IP phone security configurations will be modified to disable signaling and media encryption (including encryption provided by the VPN phone feature).

Caution Be sure to back up your system data before starting the software upgrade process.

Note We recommend that you install and assign the Cisco Unified CM "vcs-interop" SIP Normalization script to make secure calls between CTS endpoints and endpoints and devices registered to VCS.
For more information about the conditions required for secure calls, see this document:

http://www.cisco.com/en/US/docs/telepresence/cts_admin/1_8/release/notes/cts_1_8_release_notes.html#wp138743
For more information about the Cisco Unified CM script, see this document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/rel_notes/8_6_2/cucm-rel_notes-862.html#wp1961382
For more information about configuring Cisco Unified CM and Cisco VCS to interoperate via a SIP trunk, see this document:

http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Cisco_Unified_Communications_Manager_Deployment_Guide_CUCM_6-1_7_8_and_X7-0.pdf

Note If you are upgrading your software on HP 7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager. To perform an upgrade on one of these machines you must use an externally powered 16GB USB device to facilitate data migration from the old system to the new installation. For Unity Connection and Business Edition 5000, a 128GB external USB device is required. It is recommended to use an externally powered USB drive as other drives may not be recognized during the Refresh Upgrade sequence."

Consider the following notes:

- A non-bootable image is available for download from Cisco.com. This image may be downloaded to a network server (remote source) or burned to DVD (local source) and used for upgrades. DVDs that are ordered from Cisco are bootable and may be used for fresh installs.
- If you are performing a Refresh Upgrade from a version prior to Release 8.6(x) on HP7825H3 or HP7828H3 hardware, there is no option to revert to the previous version of Cisco Unified Communications Manager.
- If you do not back up your system data before starting the software upgrade process, your data will be lost if your upgrade fails.
- If you chose to revert to the prior version, you will need to install the prior version and restore your data from your DRS backup.

Cisco recommends that you locate your installation disks and licence information for the previous version to facilitate the recovery, if necessary. For more information, see the *Disaster Recovery System Administration Guide for Cisco Unified Communications Manager*.

Interoperability Between Cisco TelePresence System Endpoints And Other Devices

Prior to Cisco Unified Communications Manager Release 9.0(1), to make secure calls between Cisco TelePresence System endpoints and endpoints and devices that are registered to Cisco TelePresence Video Communication Server, Cisco recommended that you install the Unified Communications Manager vcs-interop SIP normalization script.

If you are upgrading to Cisco Unified Communications Manager Release 9.x from Release 8.5(x), and you had previously created/imported a SIP Normalization Script for VCS interoperability, the upgrade to 9.x will

fail if the name of the SIP Normalization Script used in your previous release is vcs-interop. In this case, you must rename the old script prior to completing the upgrade.

Software Upgrade Considerations

This section contains the following topics:

- Overview of Software Upgrade Process, on page 10
- Upgrading on a Virtual Server, on page 10
- Configuration Changes During Upgrade, on page 11

Overview of Software Upgrade Process

In addition to providing detailed upgrade considerations and prerequisite information, the *Upgrade Guide for Cisco Unified Communications Manager* also provides an overview of the upgrade process. Cisco recommends that you use that document as a reference before and during the upgrade process.

You must follow a specific order when upgrading Unified Communications Manager and IM and Presence Service. The order depends on the release from which you are upgrading. The preupgrade release determines the type of upgrade you must perform. There are two types of upgrades:

- Standard Upgrade
- Refresh Upgrade

Important

- Install the software during off-peak hours or during a maintenance window to avoid impact from interruptions.
- For a short period of time after you install Cisco Unified Communications Manager or switch over after upgrading to a different product version, settings changes made by phone users may be lost. Examples of phone user settings include call forwarding and message waiting indication light settings. This can occur because Cisco Unified Communications Manager synchronizes the database after an installation or upgrade, which can overwrite phone user settings changes.

Caution After you install a new node in an existing cluster, all phones that are registered to the cluster are reset.

Upgrading on a Virtual Server

If you run Cisco Unified Communications Manager on a virtual server, and are upgrading to the latest release, you must make sure that the virtual server Guest Operating System and RAM meet the requirements for the latest release.

Note In Unified Communications Manager Release 9.1, the following changes have been made to the OVAs:

- The number and the size of the vDisk for the 7500 user and 10000 user OVAs have changed from 2 x 80 GB to 1 x 110 GB. If your current VM uses the original disk sizes, do not change the size or number of disks (keep the originals in place).
- The number of vCPU for the 2500 Limited User OVA has changed from 1 vCPU to 2 vCPU.

For more information about virtual machine configurations for Unified Communications Manager Release 9.1(1), see the documentation at the following URL: http://docwiki.cisco.com/wiki/Virtualization_for_Cisco_Unified_Communications_Manager_(CUCM).

Follow this procedure to upgrade Unified Communications Manager on a virtual server:

Note These steps apply only to a Refresh Upgrade.

1. Upgrade Unified Communications Manager on the virtual machine to the latest release. For information about installing or upgrading Unified Communications Manager on virtual servers, see *Cisco Unified Communications Manager on Virtualized Servers* here http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html.
2. After you finish the upgrade, shut down the virtual machine.
3. Change the Guest Operating System to Red-Hat Enterprise Linux 5 (32-bit).
4. Check the RAM on the virtual machine and make sure that it meets the minimum RAM requirements for this release. See the readme file that accompanied this release's OVA file for minimum RAM requirements at: Products\Voice and Unified Communications\IP Telephony\Call Control\Cisco Unified Communications Manager (CallManager)\Cisco Unified Communications Manager Version [Release]\Unified Communications Manager Virtual Machine Templates.
5. Save changes.
6. Restart the virtual machine.

Configuration Changes During Upgrade

The *Upgrade Guide for Cisco Unified Communications Manager* describes restrictions that apply to the configuration changes that you can make during an upgrade. For more information, see the following URL:

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

Supported Upgrades

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

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

Note All nodes within a single cluster must be in the same mode. For example, Cisco Unified Communications Manager and IM and Presence Service nodes in the same cluster must either all be in unrestricted mode or all be in restricted mode.

Upgrade File

Before you begin the upgrade process, you must obtain the appropriate upgrade file. For base releases such as 9.0(1), you must order the upgrade file that is required using the Product Upgrade Tool (PUT) at the following URL: www.cisco.com/upgrade.

For all subsequent 9.x releases, the required upgrade file will be posted to the Downloads section of Cisco.com. You can access the upgrade file during the installation process from either a local DVD or from a remote FTP or SFTP server.

Note Be aware that directory names and filenames that you enter to access the upgrade file are case sensitive.

Upgrade Media

To upgrade to the latest release of Unified Communications Manager from a release prior to 8.0(1), use the Product Upgrade Tool (PUT) to obtain a media kit and license or purchase the upgrade from Cisco Sales.

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

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

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

Also, see the “Software Upgrades” chapter of the *Upgrade Guide for Cisco Unified Communications Manager*.

Software Upgrade Procedures

Install the COP File

Note For both restricted and unrestricted upgrades from an 8.5(x) or earlier release to a 9.0 or 9.1 release, this patch (COP file) must be applied prior to initiating the upgrade.

Procedure

	Command or Action	Purpose
Step 1	Before you upgrade from compatible versions of Unified Communications Manager, install the COP file named ciscocm.refresh_upgrade_v1.1.cop.sgn that you can find under **Cisco Unified Communications Manager Version (9.0 or 9.1)** > **Unified Communications Manager / CallManager / Cisco Unity Connection Utilities** > **COP-Files**.	

Upgrade to Restricted or Unrestricted Unified Communications Manager

If upgrading from 8.5(1) or earlier, complete the procedure Install the COP File, on page 12.

Note The unrestricted version of Unified Communications Manager is available in limited markets only.

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

Upgrade From a Local Source

Follow this procedure to upgrade the software from a local DVD.

Procedure

Step 1 For an upgrade from 8.5(1) or earlier, complete the procedure Install the COP File, on page 12.

Step 2 For a Refresh Upgrade on HP7825H3 or HP7828H3 hardware from a version prior to Release 8.6(x), use an externally powered USB disk drive with a minimum size of 16 GB to migrate the data from the old system to the new installation. For Unity Connection and Business Edition 5000, an externally powered USB disk drive with a minimum size of 128 GB is required. Cisco recommends that you use an externally powered USB drive, because other drives may not be recognized during the Refresh Upgrade sequence.

Caution If you are upgrading your software on HP7825H3 or HP7828H3 hardware from a version prior to Release 8.6(x), there is no option to revert to the previous version of Cisco Unified Communications Manager. If you do not back up your system data before starting the software upgrade process, your data will be lost if your upgrade fails. If you chose to revert to the prior version, you must install the prior version and restore your data from your DRS backup.

Step 3 If you do not have a Cisco-provided upgrade disk, create an upgrade disk by burning the upgrade file that you downloaded onto a DVD as an ISO image.

Note Copying the .iso file to the DVD will not work. Most commercial disk-burning applications can create ISO image disks.

Step 4 Insert the new DVD into the disc drive on the local server that you want to upgrade.

Step 5 Sign in to Cisco Unified Communications Operating System Administration.

Step 6 Navigate to **Software Upgrades** > **Install/Upgrade**.
The **Software Installation/Upgrade** window appears.

Step 7 From the Source list, choose DVD.

Step 8 Enter a slash (/) in the **Directory** field.

Step 9 To use the Email Notification feature, enter your Email Destination and SMTP Server in the provided fields.

Step 10 To continue the upgrade process, click **Next**.

Step 11 Choose the upgrade version that you want to install and click **Next**.

Step 12 In the next window, monitor the progress of the download.

Step 13 To run the upgraded software at the completion of the upgrade process and automatically reboot to the upgraded partition, choose **Switch to new version after upgrade**. The system restarts and is running the upgraded software. For a Refresh Upgrade on HP7825H3 or HP7828H3 hardware from a version prior to Release 8.6(x), there is no option to revert to the previous version of Cisco Unified Communications Manager, and you will not be able to choose Switch to new version after upgrade.

Step 14 To install the upgrade and then manually switch to the upgraded partition at a later time, perform the following steps, choose **Do not switch to new version after upgrade**.

Step 15 Click **Next**. For a Refresh Upgrade, the following text appears:

- For non-HP7825H3/HP7828H3 hardware:
  ```
  A Refresh Upgrade requires that you reboot the server during the
  upgrade. Services will be affected during the upgrade operation. Click
  OK to proceed with the upgrade.
  ```
- For HP7825H3/HP7828H3 hardware:
  ```
  If you are upgrading from a version prior to Release 8.6(x), this
  server model requires a USB storage device in order to proceed with
  the upgrade. Use a USB storage device with at least 16 GB of capacity.
  Note that any existing data on the USB device will be deleted.
  ```
  For Cisco Unity Connection and Cisco Business Edition 5000, the USB storage device must be at least 128 GB.

The **Upgrade Status** window displays the Upgrade log.

Step 16 After the installation completes, click **Finish** (not applicable for Refresh Upgrades).

Step 17 To restart the system and activate the upgrade, choose **Settings** > **Version**; then, click **Switch Version**.
The system restarts and runs the upgraded software (not applicable for Refresh Upgrades).

Upgrade From a Remote Source

Caution If you are performing a Refresh Upgrade on HP7825H3 or HP7828H3 hardware from a version earlier than Release 8.6(x), there is no option to revert to the previous version of Cisco Unified Communications Manager. If you do not back up your system data before starting the software upgrade process, your data will be lost if your upgrade fails. If you chose to revert to the prior version, you must install the prior version and restore your data from your DRS backup.

Supported SFTP Servers

Cisco allows you to use any SFTP server product but recommends SFTP products that are certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified versions of Cisco Unified Communications Manager. For information about which vendors certified their products with your version of Cisco Unified Communications Manager, see the following URL:

www.cisco.com/go/ctdp.

Cisco uses the following servers for internal testing. You may use one of these servers, but you must contact the vendor for support:

- Open SSH (http://sshwindows.sourceforge.net/)
- Cygwin (http://www.cygwin.com/)
- Titan (http://www.titanftp.com/)

Cisco does not support using the SFTP server product freeFTPd because of the 1 GB file size limit on this SFTP product.

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

Follow this procedure to upgrade the software from a network location or remote server.

Note Do not use the browser controls, such as Refresh/Reload, while you are accessing Cisco Unified Communications Operating System Administration. Instead, use the navigation controls that are provided by the interface.

1. If upgrading from 8.5(1) or earlier, complete the procedure Install the COP File, on page 12.
2. If you are performing a Refresh Upgrade on HP7825H3 or HP7828H3 hardware from a version prior to Release 8.6(x), use an externally powered USB disk drive with a minimum size of 16 GB to migrate the data from the old system to the new installation. For Cisco Unity Connection and Cisco Business Edition 5000, an externally powered USB disk drive with a minimum size of 128 GB is required. Cisco recommends that you use an externally powered USB drive because other drives may not be recognized during the Refresh Upgrade sequence.
3. Put the upgrade file on an FTP or SFTP server that the server that you are upgrading can access.

4 Log in to Cisco Unified Communications Operating System Administration.

5 Navigate to **Software Upgrades** > **Install/Upgrade**.

The Software Installation/Upgrade window displays.

6 From the Source list, choose **Remote File system**.

7 In the **Directory** field, enter the path to the directory that contains the patch file on the remote system.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash (/) at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter /patches.

If the upgrade file is located on a Windows server, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax. Begin the path with a forward slash and use forward slashes throughout the path. The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).

8 In the **Server** field, enter the server name or IP address.

9 In the **User Name** field, enter the user name on the remote server.

10 In the **User Password** field, enter the password on the remote server.

11 Select the transfer protocol from the **Transfer Protocol** field.

12 To use the Email Notification feature, enter your Email Destination and SMTP Server in the fields provided.

13 To continue the upgrade process, click **Next**.

14 Choose the upgrade version that you want to install and click **Next**.

15 In the next window, monitor the progress of the download.

Note If you lose your connection with the server or close your browser during the upgrade process, you may see the following message when you try to access the Software Upgrades menu again:

```
Warning: Another session is installing software, click Assume Control
to take over the installation.
```

If you are sure you want to take over the session, click **Assume Control**.

If Assume Control is not displayed, you can also monitor the upgrade with the Cisco Unified Real-Time Monitoring Tool.

16 If you want to install the upgrade and automatically reboot to the upgraded software, choose **Switch to new version after upgrade**. The system restarts and runs the upgraded software.

17 If you want to install the upgrade and then manually switch to the upgraded software at a later time, choose **Do not switch to new version after upgrade**.

18 Click **Next**. For a Refresh Upgrade, the following text appears:

- For non- HP7825H3/HP7828H3 hardware:

  ```
  A Refresh Upgrade requires that the server be rebooted during the
  upgrade. Services will be affected during the upgrade operation.
  Press OK to proceed with the upgrade.
  ```

- For HP7825H3/HP7828H3 hardware:

```
This server model requires a USB storage device in order to proceed
with the upgrade. Use a USB storage device with at least 16 GB of
capacity. Note that any existing data on the USB device will be
deleted. For Cisco Unity Connection and Cisco Business Edition the
USB storage device must be at least 128 GB.
```

The **Upgrade Status** window displays the Upgrade log.

19 When the installation completes, click **Finish** (not applicable for Refresh Upgrades).

20 To restart the system and activate the upgrade, choose **Settings** > **Version** then click **Switch Version**.

The system restarts running the upgraded software (not applicable for Refresh Upgrades).

Bridge Upgrade

The bridge upgrade provides a migration path for customers who want to migrate from a discontinued Cisco Unified Communications Manager server to a server that supports the newest release of Cisco Unified Communications Manager. For more information, see the *Upgrade Guide for Cisco Unified Communications Manager* here: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html.

Post-Upgrade Tasks

After the upgrade, perform the postupgrade tasks that are outlined in the *Upgrade Guide for Cisco Unified Communications Manager*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html. Refer also to the Important Notes section of this document for additional information. Note that you must perform the following post-upgrade tasks only after you complete the upgrade for the entire cluster and set up the database:

- Install additional locales
- Install COP files

Note After you perform a switch version when you upgrade Unified Communications Manager, IP phones request a new configuration file. This request results in an automatic upgrade to the device firmware.

Latest Software and Firmware Upgrades

After you install or upgrade to this release of Unified Communications Manager, check to see whether Cisco has released software upgrades, firmware upgrades, critical patches, or Service Updates.

Firmware

Apply the latest comprehensive Firmware Upgrade CD (FWUCD) as soon as possible to help prevent catastrophic failures.

To check for the latest FWUCD from www.cisco.com, perform the following steps:

1 Select **Support** > **Download Software**.

2 Navigate to **Products** > **Voice and Unified Communications** > **Communications Infrastructure** > **Voice Servers** > **Cisco 7800 Series Media Convergence Servers (or Cisco UCS B-Series Blade Servers)** > ***(your server model)***.

Software

Service Updates (SUs) contain fixes that were unavailable at the time of the original release. They often include security fixes, firmware updates, or software fixes that could improve operation.

To check for software upgrades, SUs, and critical patches from www.cisco.com, perform the following steps:

1 Select **Support** > **Download Software**.

2 Navigate to the "Voice and Unified Communications" section and select **IP Telephony** > **Call Control** > **Cisco Unified Communications Manager (CallManager)** > ***the applicable version of Cisco Unified Communications Manager for your deployment***.

Related Documentation

You can view documentation that is associated with supported applications.

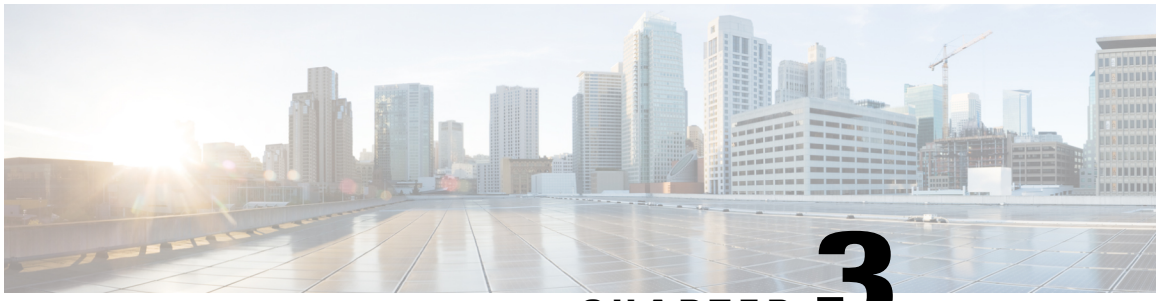
Application	Documentation Link
Cisco Unified Communications Manager	http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html
Cisco Unified Contact Center Express	http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/tsd-products-support-series-home.html
Cisco Unity Connection	http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/tsd-products-support-series-home.html

Limitations and Restrictions

For a list of software and firmware versions of IP telephony components and contact center components that were tested for interoperability with this release of Unified Communications Manager as part of Cisco Unified Communications System testing, see the following web page:

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

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



CHAPTER 3

Upgrading to IM and Presence Release 9.0(1)

- New system installation information, page 21
- System Upgrade, page 21
- Upgrade order, page 23
- Software licensing requirements for VMware, page 23
- Recommendations for release 8.0(x), 8.5(x), or 8.6(x) to 9.0(1) upgrades, page 23

New system installation information

For new installations, you must order the IM and Presence Service system software and adhere to licensing requirements. To order the software, go to http://www.cisco.com/en/US/ordering/index.shtml or contact your Cisco sales representative.

Each IM and Presence Service shipment comes with an installation DVD, which is required for all new installations of IM and Presence Service. The IM and Presence Service operating system and application software is installed from the installation DVD. For example, for new installations of IM and Presence Service software, use the DVD that indicates this release of IM and Presence Service.

Note If you fresh install the unrestricted version of IM and Presence Service Release 10.0(1), you will not be able to later perform a fresh install of the restricted version of this software.

System Upgrade

Supported upgrade paths to IM and Presence Release 9.0(1)

IM and Presence supports the following software upgrade paths to Release 9.0(1):

Supported Upgrade Paths from IM and Presence...	Installation Instructions
Release 8.0(1) through 8.6(4) to 9.0(1) **Note** Upgrading from Cisco Unified Presence Release 8.6(5) and later to IM and Presence Release 9.0(1) is not supported.	Upgrades from Release 8.0(1) through 8.6(1) to Release 9.0(1) require a Refresh Upgrade using the UCSInstall_CUP_*.sgn.iso file. Upgrades from Release 8.6(2) and 8.6(3) to Release 9.0(1) require a Refresh Upgrade only. Upgrades from Release 8.6(4) to Release 9.0(1) require a Standard Upgrade only. **Note** For more information about Refresh Upgrades and Standard Upgrades, see the *Upgrade Guide for Cisco Unified Communications Manager, Release 9.0(1)*. Perform these steps to proceed with the upgrade: **1** Go to http://www.cisco.com/cisco/software/navigator.html. **2** Navigate to **Products** > **Voice and Unified Communications** > **Unified Communications Applications** > **Cisco Unified Presence** > **Cisco Unified Communications Manager IM and Presence Service Version 9.0** > **Unified Presence Server (CUP) Updates-9.0(1)**. **3** Download the complete ISO file: UCSInstall_CUP_9.0.1.10000-21.sgn.iso

Note Direct upgrades from Cisco Unified Presence Release 6.0(x) to Release 9.0(1) are not supported. You must first upgrade to at least Release 8.0(1) of Cisco Unified Presence. For more information about upgrading to Cisco Unified Presence Release 8.x, see the Release Notes for Cisco Unified Presence here on Cisco.com: http://www.cisco.com/en/US/products/ps6837/prod_release_notes_list.html.

Upgrade from Cisco.com

Cisco does not support downloading major IM and Presence Service software releases from Cisco.com, for example, IM and Presence Service Release 9.0(1). You can download from Cisco.com upgrade-only software images that are used to upgrade from a previous major software release to a subsequent software maintenance release or point release of IM and Presence Service. For example, you can download Cisco Unified Presence Release 8.0(2) or Cisco Unified Presence Release 8.6(1) from Cisco.com.

To download this software, go to http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240. You must have an account on Cisco.com to access the Software Center. The images that are posted at the Software Center require existing installations of IM and Presence Service.

Upgrade order

You must follow a specific order when upgrading Unified Communications Manager and IM and Presence Service. The order depends on the release from which you are upgrading. The preupgrade release determines the type of upgrade you must perform. There are two types of upgrades:

- Standard Upgrade
- Refresh Upgrade

For more information about these types of upgrades and the upgrade order that you must follow for each type, see the latest version of the *Upgrade Guide for Cisco Unified Communications Manager* here: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html.

Software licensing requirements for VMware

You can run this release of IM and Presence Service on a VMware virtual machine that is deployed on approved Cisco Unified Computing server hardware. For information about supported servers, see *Hardware and Software Compatibility Information for IM and Presence Service on Cisco Unified Communications Manager*. For information about the VMware licensing requirements, see the License Activation for Cisco Unified Communications on Cisco Unified Computing System Docwiki here: http://docwiki.cisco.com/wiki/License_Activation_for_Cisco_UC_on_UCS.

Recommendations for release 8.0(x), 8.5(x), or 8.6(x) to 9.0(1) upgrades

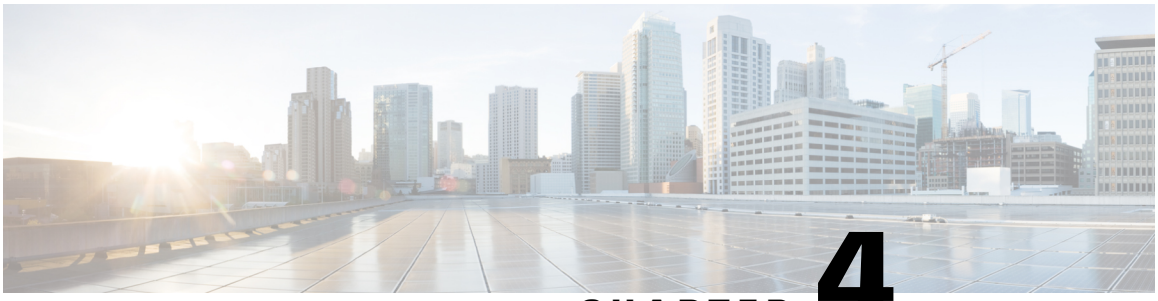
Before you upgrade from Cisco Unified Presence Release 8.0(x), 8.5(x), 8.6(x) to IM and Presence Service Release 9.0(1), Cisco strongly advises that you follow the recommended upgrade procedure in the *Upgrade Guide for Cisco Unified Communications Manager, Release 9.0(1)* here: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html.

Important Notes

- Cisco Unified Presence Sync Agent Service-prior to performing an upgrade, this service may be disabled on the cluster (which only runs on the Publisher node). This will ensure that user-initiated changes from the corresponding Unified Communications Manager system during the upgrade, do not compromise the upgrade process. The changes will be reconciled when the IM and Presence Service Sync Agent is restarted in either the current or newer version.
- Publisher node-switch versions and restart the publisher node prior to initiating a switch version and restart on the Subscriber nodes. If the IM and Presence Service Administration GUI is operational on the Publisher node, it is safe to initiate a switch version and restart on the Subscriber node.

Note Services on the Publisher will not start until the Subscribers are switched, restarted, and replication is successfully established on that cluster.

- High Availability User Support-Cisco Unified Presence Release 8.6(1) supports up to 15,000 users per cluster in a High Availability (HA) configuration and up to 30,000 users per cluster in a non-HA configuration. If, when you upgrade, you are left with a number of unsupported users, Cisco recommends that you unlicense these surplus users on Unified Communications Manager before you perform the upgrade.
- Contact List Size-the default maximum value is 200; however you can configure this to a higher value, or configure 0 to set it to unlimited value. After you perform the upgrade, check that the contact list size for users has not reached the maximum value. If you have a large number of contacts per user, the number of users that a IM and Presence Service node supports is reduced.



CHAPTER 4

Important Notes

The following sections contain important information that may have been unavailable upon the initial release of documentation for Unified CM and IM and Presence Release 9.0(1).

- Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets, page 26
- Cisco Unified Mobility Disclaimer, page 26
- Configure LDAP Directory, page 26
- DoCoMo Phones Not Certified, page 27
- Install Language Prompts for TAPS, page 27
- IPv4-Only Support for Video Streams, page 27
- Jabber Certificate Warnings with IM and Presence Service, page 28
- LBM Hub Node TCP Port 9004 Must Only Be Accessible by Trusted Nodes, page 28
- Locale Installer Locale File for Belgium, page 28
- Localization Not Supported for Some Unified CM Components, page 28
- RD Numbers Cannot Be Provisioned on Two Different Clusters, page 29
- Unified CM Assigns a Nonsecure Conference Bridge When the Conference is Initiated by a Nonsecure Phone, page 29
- Upgrade Restores Configure Automatic Database Purge Parameter Default, page 29
- Devices Reset while Certificate Regeneration, page 29
- MGCP IOS Gateway From PSTN Does Not Support Connected Address in ISDN Notify , page 29
- Perfect Forward Secrecy is not Supported in IPsec Configuration, page 30
- Change Perfmon Counter File Size Parameters in RTMT, page 30

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.

Configure LDAP Directory

You can add users from your corporate directory to the Cisco Unified Communications Manager database by synchronizing the user data to the database. Cisco Unified Communications Manager allows synchronization from the following directories to the database:

Note This is an updated list for this release.

- Microsoft Active Directory 2000
- Microsoft Active Directory 2003 R1 & R2 (32-bit)
- Microsoft Active Directory 2008 R1 (32-bit) & R2 (64-bit)
- Microsoft Active Directory Application Mode 2003 R1 & R2 (32-bit)
- Microsoft Lightweight Directory Services 2008 R1 (32-bit) & R2 (64-bit)
- Sun ONE Directory Server 5.2
- Sun ONE Directory Server 6.x
- Oracle Directory Server Enterprise Edition 11gR1
- OpenLDAP 2.3.39
- OpenLDAP 2.4

DoCoMo Phones Not Certified

This information applies to CSCua87279.

The Remote Destination Configuration Settings section that appears in the "Cisco Unified Mobility" chapter of the *Cisco Unified Communications Manager Features and Services Guide* states that the Mobile Phone check box does not apply to dual-mode phones that are running SIP, such as DoCoMo N902iL and DoCoMo N906i. This information is correct. However, the DoCoMo phones should not be explicitly mentioned since neither phone has been certified with Cisco Unified Communications Manager.

Install Language Prompts for TAPS

If you need to install language prompts other than English, you must install the Locale Installer on all nodes in your Unified CM cluster. After you install the Locale Installer, you must pull the locale specific AAR file that the Locale Installer saves to the Unified CM TFTP directory and install that file in Cisco Unified Contact Center Express.

Procedure

Step 1 Download the Locale Installer that contains your language from cisco.com.

Step 2 Install the Locale Installer on each Unified CM cluster node.

Note For detailed installations on installing locales in Unified CM, see "Software Upgrades" in the *Cisco Unified Communication Operating System Administration Guide*.

Step 3 Restart each cluster node.

Step 4 Login to Cisco Unified Operating System Administration and choose **Software Upgrades** > **TFTP File Management**.

Step 5 Search for the AAR file that the Locale Installer installed in Unified CM's TFTP directory.

Step 6 Login to Cisco Unified Operating System CLI.

Step 7 Use the **file get tftp <AAR file name>** CLI command to get the file from Unified CM's TFTP directory.

Step 8 See the Cisco Unified Contact Center Express product documentation for instructions on how to install and configure the AAR file in Cisco Unified Contact Center Express.

IPv4-Only Support for Video Streams

Cisco Unified Communications Manager Release 9.0 supports IPv4 only for video streams. Calls between video endpoints and an application must use IPv4 only for both voice and video media streams.

Before Cisco Unified Communications Manager Release 9.0, there was one exception. Cisco Unified Video Advantage, which uses IPv4 exclusively, could be associated with a dual-stack Skinny Client Control Protocol (SCCP) IP phone, forming a composite endpoint which could, in certain circumstances, use IPv6 for voice and, at the same time, IPv4 for video media streams.

In Cisco Unified Communications Manager Release 9.0 and later, this exception is no longer supported, and video will be disabled whenever a dual-stack IP phone configured in dual-stack or IPv6-only mode is associated

with Cisco Unified Video Advantage. IP phones associated with Cisco Unified Video Advantage must be reconfigured to use IPv4 only for voice, if they are to continue to support video.

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.

LBM Hub Node TCP Port 9004 Must Only Be Accessible by Trusted Nodes

Unified CM 9.0(1) introduces a new architecture for propagating Locations Bandwidth information end-to-end in a multi cluster environment. In the initial release, this feature is not secured so it is critical that only trusted hosts are able to access TCP Port 9004 on any node configured as a Locations Bandwidth Manager (LBM) Hub Node. Future versions of Unified CM will implement a solution to verify the authenticity of this signaling. This requirement does not apply for isolated clusters with no LBM Hub Node Groups configured.

Locale Installer Locale File for Belgium

This information applies to CSCua01779.

Because the primary language spoken in Belgium is Dutch, you can download the Dutch (Netherlands) locale file, for example, cm-locale-nl_NL- 8.5.1.2100-1.cop.sgn (Cisco Unified Communications Locale Installer 8.5.1.21000-1 Dutch (Netherlands)). Secondary languages commonly spoken in Belgium are French and German.

Localization Not Supported for Some Unified CM Components

Localization is not supported for the following Cisco Unified Communications Manager, Release 9.0(1) components:

- Cisco Unified Serviceability
- Cisco Unified Reporting Tool
- Cisco Disaster Recovery System
- Cisco Dialed Number Analyzer

Note Cisco Unified CM Administration is localized for Japanese, Chinese, and Korean; **Cisco Unified CM Administration** > **Help** only supports Japanese.

RD Numbers Cannot Be Provisioned on Two Different Clusters

The same RD cannot be provisioned on two different clusters. If a call is made across two clusters, the dtmf signal, and some other signals, will stop forwarding after hitting the first provisioned RD cluster. The second cluster will not receive it.

Unified CM Assigns a Nonsecure Conference Bridge When the Conference is Initiated by a Nonsecure Phone

If a nonsecure phone that is assigned to a media resource group list initiates a conference and a nonsecure conference bridge is available in the media resource group list, Cisco Unified Communications Manager allocates the nonsecure conference bridge even if a secure conference bridge with a higher priority ranking is also available in the media resource group list.

Upgrade Restores Configure Automatic Database Purge Parameter Default

Following an upgrade, the Configure Automatic Database Purge > MAX DATABASE AGE parameter will be changed to one of the following:

- If the MAX DATABASE AGE in the old version is between 1 and 60, it will be configured to 60 in the new version.
- If the MAX DATABASE AGE in the old version is between 60 and 180, it will be configured to the same age in the new version.
- If the MAX DATABASE AGE in the old version is more than 180, it will be configured to 180 in the new version.

Devices Reset while Certificate Regeneration

This update is applicable for CSCus63274.

With CIA 2541, all the devices (phones) reset when you regenerate TVS/ CCM/ 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.

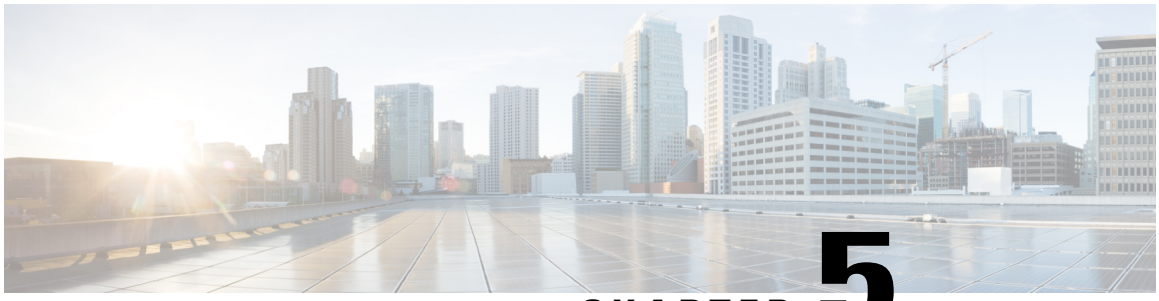
Perfect Forward Secrecy is not Supported in IPsec Configuration

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.



CHAPTER 5

New and Changed Information

The following sections describe new features and changes that are pertinent to IM and Presence Release 9.0(1). The sections may include configuration tips, information about users, and where to find more information.

Note For feature-related information pertaining to Unified CM, see the *New and Changed Information for Cisco Unified Communications Manager, Release 9.0(1)* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html

- Integration of Unified CM and IM and Presence, page 31
- Deprecated Features, page 32
- Licensing, page 32

Integration of Unified CM and IM and Presence

Unified CM and the IM and Presence Service are more closely integrated in release 9.0(1). This integration improves the installation and configuration experience for administrators. Here is a list of changes implemented in this release:

- Unified CM and the IM and Presence service must be upgraded in the same maintenance window and both versions (major and minor) must align. Major and minor release numbers are defined as follows:

  `9.x.y`

  where: `9` = major release number, `x` = minor release number and `y` = maintenance release number.

- All Unified Communications user and service configuration in Cisco Unified Presence Release 8.x has moved to Unified CM 9.0 and will be centrally configured on Unified CM from release 9.0 on. This data is automatically migrated to Unified CM during upgrade of Cisco Unified Presence release 8.x to IM and Presence release 9.0.
- Server and client licensing requirements have moved from IM and Presence to Unified CM.

Deprecated Features

The IM and Presence Service does not support the following:

- IP Phone Messenger (IPPM)
- Cisco Unified Personal Communicator Release 7.x

Licensing

The Licensing system, specifically the License Usage Report, has been revised to track and report on the usage and consumption of licenses on a per-user basis and unassigned device by device type. Licenses are now installed on the Enterprise License Manager and are no longer installed on the Cisco Unified Communications Manager. For more information, see the "Licensing" chapter of the *Cisco Unified Communications Manager Features and Services Guide*.

Enterprise License Manager introduces centralized license fulfillment and management that collects license usage information for all connected publishers or servers, and compares them to the licenses installed on the Enterprise License Manager. The following functionality is introduced as part of Enterprise License Manager:

- License migration utility – automatically migrates pre-Release 9.0 installed licenses once a system with pre-Release 9.0 installed licenses is upgraded to 9.0(1). The License Migration Utility bases its calculations on current configuration information (users, devices per user, and unassigned devices) and carries forward unused phone unit (device license units) licenses for use for conversion to 9.0 licenses.
- License sharing – available licenses are shared between connected product instances to meet the total license requirements
- Tiered license substitution – available higher level licenses are loaned to meet lower level license requirements

For more information, see the *Enterprise License Manager User Guide*.

Introduces Advanced User Connect License (not made commercially available). The following devices require Advanced User Licenses in 9.0(1):

- Cisco IP Communicator
- Cisco Unified Personal Communicator
- Carrier-Integrated Mobile
- Unified Client Services Framework
- Cisco Telepresence EX60
- Cisco Telepresence EX90

Cisco Unified Workspace License (UWL) Standard is allowed for up to two devices per user.

UWL Premium License (not made commercially available) is introduced. The following devices require UWL Premium Licenses in 9.0(1):

- Cisco Dual Mode for Android

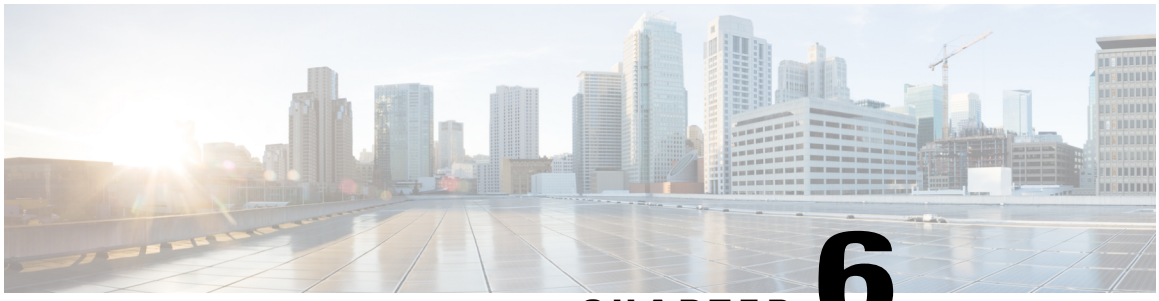
- Cisco Dual Mode for iPhone
- Cisco Unified Mobile Communicator
- IMS-integrated Mobile

Important Software feature and node licenses are no longer applicable as of 9.0(1).

Single Screen and Multi Screen TelePresence licenses are no longer applicable and have been combined with one TelePresense Room License that applies for all immersive and multi-purpose TelePresence devices.

The following license types are no longer applicable:

- UWL Entry
- UWL APAC
- Adjunct UCL
- Public space UCL
- Video desktop UCL
- Mobile UCL
- Hotel UCL



CHAPTER 6

Caveats

- Bug Fixes and Updates, page 35
- Bug Search Tool, page 35
- Resolved Caveats, page 36
- Open Caveats, page 36

Bug Fixes and Updates

For the latest bug fixes, we recommend that you upgrade to Release 9.1(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 CM Release 9.0 and IM and Presence Release 9.0:

- Open Caveats for Unified CM Release 9.0(1), on page 37
- Open Caveats for IM and Presence Release 9.0(1), on page 48

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

Understanding the Fixed-in Version Field in the Online Defect Record

When you open the online record for a defect, you will see data in the "First Fixed-in Version" field. The information that displays in this field identifies the list of interim versions in which the defect was fixed. These interim versions then get integrated into Unified CM 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 you can decode the maintenance release interim version information. These examples show you the format of the interim version along with the corresponding Unified CM release that includes that interim version. You can 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 for Unified CM Release 9.0(1), on page 37 and Open Caveats for IM and Presence Release 9.0(1), on page 48 reflect a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit and follow the instructions as described in the Bug Search Tool, on page 35.

Open Caveats for Unified CM Release 9.0(1)

The following table lists open caveats which may cause unexpected behavior in Unified CM 9.0(1).

Table 3: Open Caveats for Unified CM

Identifier	Severity	Component	Headline
CSCtz93804	3	axl	updateSNMPUser and addSNMPUser changes are not reflected by the GUI
CSCtz76050	3	axl	AXL takes over 2 minutes to recover after lost connection to publisher
CSCtz23557	3	axl	SOAP handler sends response in an exception handler.
CSCua28859	3	axl	SCCP C881VA-V and C887VA-V gateway port registration
CSCua23787	3	backup-restore	DRS Exception if SFTP Server Down
CSCua14976	3	bat	Unable to upload BAT files with Safari on Mac
CSCua19534	3	bps-bat	BAT can not insert 10K remote destinations

Identifier	Severity	Component	Headline
CSCua24313	2	car	Upgrade fails due to missing CAR PID.
CSCty20488	2	ccmcip	Throttle the number of connections to the database from Cisco CallManager Cisco IP Phone (CCMCIP) service.
CSCtz81147	2	ccm-serviceability	Unable to control the subscriber from the publisher ccmservice pages.
CSCua18601	3	ccm-serviceability	SNMP trap is not sent.
CSCua18514	3	ccm-serviceability	Buttons are clickable even if they are greyed out on Serviceability page.
CSCua24582	3	ccm-serviceability	session trace tool doesnt show Aside call-leg when call traverses nodes
CSCtz95192	3	ccm-serviceability	vos alerts not getting cleared
CSCtz29859	3	ccm-serviceparam	User Control System Parameters
CSCua09290	3	cli	CLI "set password user security" did not set the correct apps password
CSCtz97055	3	cli	CLI "set network hostname <hostname>" providing wrong warning
CSCua19164	3	cmcti	CSCto54048 broke cm_8_6_2
CSCtz47156	3	cmcti	Extension Mobility load leads to CallProcessingNodeCPUPegging alert
CSCty98135	3	cmcti	CTI Remote Device not sending calling name to active Remote Destination
CSCty86117	3	cmcti	Get inconsistent value of called party URI when there are 2 URI config
CSCty20138	3	cmcti	No URI info on Join Same Line scenario with CTIRD
CSCty02858	3	cmcti	Get platform exception on transfer with multiple hold and resume
CSCty51564	3	cmui	Accessibility : Links/Dropdown are not accessible with Tab key
CSCtz90511	3	cmui	CCMUser: with multiple devices

Identifier	Severity	Component	Headline
CSCua26470	3	cmui	KOR: CUCM 9.0: java exception when finishing IPMA wizard
CSCua26049	3	cmui	UCM User page is not opening for + in the User Id
CSCua15401	3	cmui	When navigating pages
CSCtz90546	3	cmui	CCMUser: change password against LDAP user should be barred
CSCua15443	3	cmui	CCMUser: I am requested to perform an impossible action.
CSCua15453	3	cmui	CCMUser: Notifications should be actionable
CSCua17362	3	cmui	Directory Number can not begin with a "+".
CSCua17412	3	cmui	Auto Registration does not support DNs >8 digits.
CSCua18570	3	cmui	Resetting user password is not authenticated on ucmuser page
CSCua10440	3	cmui	Application user page, Find more phone result in syntax error
CSCtz95551	3	cmui	CCMAdmin: Propagate selected is broken on Safari
CSCtz89233	3	cmui	UOP users unable to configure pre-existing SD after 9.0 upgrade
CSCtz44698	3	cmui	Misleading failure message when updating directory number with URI
CSCty87428	3	cmui	Accessibility : JAWS tool reads out password for UOP on IE
CSCty65429	3	cp-cac	Annunciator oversubscription doesnt increase "OutOfResource" counter
CSCua19446	3	cp-callcontrol	Incorrect behavior on URI dial out to VCS via SIP trunk
CSCua08180	3	cp-callcontrol	Calling party URI not displayed on cross cluster transfer
CSCua21008	3	cp-callqueuing	Disable Initial Announcemnt while selecting ANN to playing ringback tone

Identifier	Severity	Component	Headline
CSCua14994	3	cp-database	When adding LDAP dir, warning displays "Existing End Users" be deleted
CSCua19800	3	cp-device-manager	New DeviceTypes use device defaults device pool that is apparently random.
CSCtz63687	3	cp-digit-analysis	SIP route pattern match fails for a specific domain name
CSCua02601	2	cp-h323	Consult Transfer call over ICT failing. JTAPI logs show "Success=no".
CSCua14268	2	cp-mediacontrol	Call transfer (Blind/Consult) does not work for Video (CUVA) calls.
CSCua02601	2	cp-mediacontrol	Consult Transfer call over ICT failing. JTAPI logs show "Success=no"
CSCua20188	3	cp-mediacontrol	CUCM not convert Skinny into RFC2833 for incoming call of IP phone 7985
CSCua15124	3	cp-mediacontrol	Ipv6 Mid Call Ip/Port change leads to call failure
CSCua08091	3	cp-mediacontrol	Send call to Mobile failure
CSCtz88952	3	cp-mediacontrol	transfer the holded call over H323GW while Multicast moh play,call drop
CSCtz86874	3	cp-mediacontrol	X-cisco-mux should be supported over MTP
CSCty94482	3	cp-mediacontrol	BW allocated is less when video is removed/re-added, but TIAS is same
CSCtw79071	3	cp-mediacontrol	Handle H323 pass thru race conditions (exposed by call queuing feature)
CSCtu36592	3	cp-mediacontrol	Handle MediaExchangeOfferRejected over PT MTP
CSCua12011	3	cp-mgcp	Calling party number is not seen in CDR report for Incoming Call.
CSCtz83878	3	cp-mobility	DTMF fails to be sent prior to a connect when EFA is enabled.
CSCua03158	3	cp-mobility	desk phone does not ring when SNR via AAR and use User Control

Identifier	Severity	Component	Headline
CSCua24406	2	cp-mobility	SNR is broken when RD is associated with Dual mode device.
CSCtz52093	3	cpi-afg	Answer file generator not complaining for unsupported passwords
CSCua25702	3	cpi-appinstall	ETSGJ-CH:Showing invalid inactive version after upgrading CUCM to 9.0
CSCua23507	3	cpi-appinstall	Clarify status message for QED cop file install on subscribers
CSCua23498	3	cpi-cert-mgmt	set web-security mishandling multiple Subject Alternative Names
CSCua20054	3	cpi-cert-mgmt	export using BulkCertMgmt shows Sftp Operation failure incorrectly
CSCtz83937	3	cpi-cert-mgmt	TFTP Certificate Mismatch btw DB and file system after DRS restore
CSCua17013	3	cpi-os	OpenSSL DTLS Vulnerability (RHSA-2012:0699-1)
CSCty39513	3	cpi-os	Sudo Privilege Escalation Vulnerability (CVE-2011-0010)
CSCtz87023	3	cpi-platform-api	Add the current owner info to the error message
CSCua24526	3	cpi-security	Subscriber Upgrade to 9.0 in FIPS mode prompts for sftpuser password
CSCty29409	3	cpi-security	CUCM GUI not working when some services are restarted while SSO enabled
CSCua25245	3	cpi-service-mgr	memory leak in servMEvtHdlr::sendMsg
CSCua22651	3	cpi-service-mgr	Service Name change
CSCua26133	3	cp-qsig	MGCP controlled E1 with Qsig not prefixing digits when transferred
CSCty85550	3	cp-qsig	Call disconnected if Auto Pickup and blind transfer prior to pickup
CSCua07917	2	cp-saf-ccd	Cluster will not advertise newly added route patterns via CCD/SAF.

Identifier	Severity	Component	Headline
CSCua09803	3	cp-sccp	Pause in Speed Dial DTMF not working for SCCP phones when HW MTP invoked
CSCua25173	3	cp-sccp	UCM indicates different DSCP for audio and video in SCCP video call
CSCtz70744	3	cp-sip-station	After answering incoming call on shared line, Cius continues to ring
CSCtz86173	3	cp-sip-station	UCM Group Apply Config does not reset phones
CSCtz70744	3	cp-sip-station	After answering incoming call on shared line
CSCty68974	3	cp-sip-station	RingTimingSet name is editable on UserPreference/User page
CSCua28141	3	cp-sip-trunk	Remote in use session will not disappear after authentication failed call
CSCtz84000	3	cp-sip-trunk	Forwarded calls hairpinned over QSIG PRI to SCCP voicemail fail
CSCtz71142	3	cp-sip-trunk	SIPProfile "Use Fully Qualified Domain Name in SIP Requests" Named wrong
CSCua26902	3	cp-sip-trunk	Fix Static Analysis issues for ProcessSIPHandler.cpp for cc_mainline
CSCua00342	3	cp-supplementaryservices	Group PickUP fails when URI contains special characters.
CSCua00351	3	cp-supplementaryservices	BLF/SD - Speed Dial fails when URI contains special characters
CSCua00366	3	cp-supplementaryservices	BLF/SD - Busy Lamp Field fails when URI contains special characters
CSCtz93914	3	database	RTMT: Reconfigure DB User Host Information Counters Alert After Upgrade
CSCtz96952	3	database	Database Replication setrepltimeout of 4500 seconds doesn't take effect
CSCua05467	3	database	CUCM hostname change does not roll back properly after failure
CSCts69714	3	database-ids	PMR 12346 - cdr define server gets error 47

Identifier	Severity	Component	Headline
CSCty16906	3	database-ids	PMR 34008 Replication not setting up repeating 213 error
CSCua12724	3	database-ids	PMR 55392 - sessions hung in ccmtemp space
CSCua19424	3	database-ids	PMR 57200 Forcedatasyncsub takes hour (up to 9!)
CSCua15589	3	directory	Why do converted LDAP end users allow LDAP authentication but new ones don't?
CSCua15131	3	directory	EX-60 problems dialing SIP URIs without specifying domain
CSCtz98464	3	e911	Location association only possible from one phone in shared line
CSCua22712	3	e911	Replace UUID based call routing with the DID based
CSCua07337	3	elm	ELM is showing the last license file as "active" in demo mode
CSCua21231	3	elm	In demo mode, bad file installed as license gives inaccurate error
CSCtz94469	3	elm	Product re-add after the hostname change provides duplicate node error
CSCtz90296	3	em-database	Softkey template in default Device Profile not used for mismatch login
CSCtz73147	3	ext-mobility	EMApp subscribes to componentversion leading to CPU spike post upgrades
CSCua24379	2	ils	ILS TLS not working with CA signed certs
CSCtz06775	3	ims	When admin locks user, that user cannot be unlocked in SSO mode
CSCtz26161	3	ims	sso enable takes more time than expected
CSCua11704	3	ims	Database Authentication take up to 40 seconds to complete
CSCty89315	3	jtapisdk	Get DisconnectedEv with wrong cause after transfer conference

Identifier	Severity	Component	Headline
CSCua19586	2	jtapisdk	NullPointerException when reconnecting to provider
CSCtz94527	3	media_str_app	MOH is played to other party during mobile connect handoff
CSCtz73077	3	personaldirectory	Fast Dials delayed when using a subscriber across the WAN from publisher
CSCtz88723	3	qrt	CEF core dump after CallManager Upgrade/Switch version
CSCty97376	3	qrt	Quality report window is not localized when the string is translated
CSCtw78204	3	rtmt	RTMT does not collect OPC Logs [OPC is a UCCE PG process]
CSCua16508	2	sa-callp	Unable to delete telwork's site.
CSCtz68603	3	sa-countrypack	CP Install from MAC Page auto reboot system without notification
CSCua16829	3	sa-docs	Online Help does not have information about "Single Number Reach Voicemail Policy".
CSCtz68637	3	sa-docs	BE3K: Failure using REACH ME ANYWHERE in Brazil E1R2
CSCua17848	2	sa-mac	Caddo: Unable to add PSTN connection T1 PRI gateway
CSCtz72524	3	sa-mac	Feature Extensions section is blank in DialPlan page in this scenario
CSCtw60961	3	sa-mac	Able to access CB3K admin page tabs before it pop-up Post Setup Wizard
CSCua63152	3	security	Login failure after converting LDAP Synchronized User to Local User
CSCty94318	3	security	Webdialer.war deployment effecting PKI cert based SSO admin login
CSCtz67616	3	security	Add selinux policy to allow execution of java as remote support user
CSCtz58963	3	selinux	Initial Selinux loading process IO impact delays server bootup

Identifier	Severity	Component	Headline
CSCua21613	3	selinux	Selinux caused a cimserver core on 8.6.1.21021-1
CSCua19164	3	tapisdk	CSCto54048 broke cm_8_6_2
CSCua29576	3	tftp	Sustained EM Login/Logout leads to delay in completing EM requests
CSCtz70136	3	tftp	TFTP needs to support addition of UC Services to DB without code change.
CSCtz84807	3	ucm-user-licensing	UCMs license usage report and ELM information
CSCtz95366	3	ucm-user-licensing	License warning on CUCM shows wrong number of days
CSCtz92247	3	uds	Phones are showing up multiple times for a given user.
CSCua21058	3	voice-sipstack	During V.150 call CUCM sends "Versn" and the V should be lower case
CSCua23592	3	voice-sipstack	CUCM unable to parse mrmods parameter in v150 SDP

Table 4: Device Licensing Caveats

Device	Description	Fix
CTI Port	CTI Port licensing in 9.0(1) consumes an Enhanced license when CTI Port should not consume any license type.	This has been fixed in 9.1(1)
Cisco 6901	Cisco 6901 phone in 9.0(1) consumes a Basic license when Cisco 6901 phone should consume an Essential license type.	This has been fixed in 9.1(1)
iOS or Android devices	When assigned to a user, iPhone, iPad and Android devices consume an additional Basic license. CSCuc11836	This has been fixed in 9.1(1)

Device	Description	Fix
Devices require UWL Premium license	The following devices consume a Cisco UWL Premium license: • Cisco Dual Mode for Android • Cisco Dual Mode for iPhone • Cisco Unified Mobile Communicator • IMS-integrated Mobile The devices should require an Enhanced license.	This has been fixed in 9.1(1)
Devices require and Advanced UCL	The following devices consume an Advanced UCL: • Cisco IP Communicator • Cisco Unified Personal Communicator • Carrier-Integrated Mobile • Unified Client Services Framework • Cisco Telepresence EX60 • Cisco Telepresence EX90 The devices should require an Enhanced license.	This has been fixed in 9.1(1)
UWL Standard maximum devices	The maximum number of devices for a Cisco UWL Standard license is up to 2 devices when the maximum number of devices should be 10.	This has been fixed in 9.1(1)

Table 5: Enterprise License Manager 9.0(1) Caveats

Device	Description	Fix
License Migration Utility	• Supports license upgrades for Cisco Unified Communications Manager Release 6.x to 8.x. • For Release 6.x to 8.x systems, licenses must be installed and recognized (as "uploaded") on the server they were originally issued to prior to Cisco Unified Communications Manager upgrade to 9.0(1). If the server MAC or License MAC changes, the license upgrade will fail. • Uninstalled DLUs and unregistered license PAKs must be fulfilled and installed prior to Cisco Unified Communications Manager upgrade to 9.0(1)	• For 5.X and pre-5.X systems, submit a case to manually upgrade your existing licenses to licensing@cisco.com • Re-host licenses and verify that they are "uploaded" on the version just prior to the upgrade to 9.0(1). • Uninstalled DLUs and unregistered PAKs cannot be installed onto ELM. Submit a case to licensing@cisco.com
Upgrades to 9.0(1) or 9.1(1)	Upgrade orders for 9.0(1) or 9.1(1) do not issue any license PAKs. License upgrades to 9.0(1) or 9.1(1) are done through the license migration utility on the Enterprise License Manager.	Use the license migration utility to migrate existing (installed) licenses to 9.0(1) or 9.1(1). From the Enterprise License Manager, go to **License Management > License Planning > Upgrade Licenses**.
Upgrades from 9.0(1) to 9.1(1)	Cisco UWL Premium and Advanced UCL licenses issued for 9.0(1) are not recognized by Enterprise License Manager 9.1(1). License files containing Cisco UWL Premium and Advanced UCL licenses must be submitted back to Cisco for replacement and re-issuance to an Enterprise License Manager 9.1(1) license file.	If your license file includes UWL Premium or Advanced UCL, contact Cisco at uc91-license@cisco.com for license file replacement.

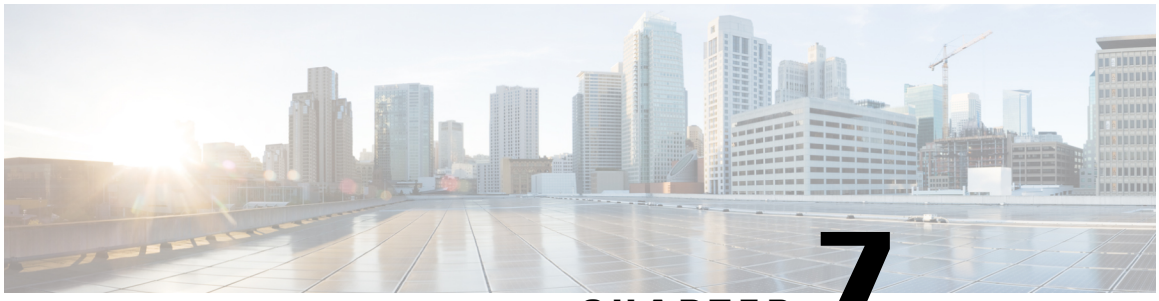
Device	Description	Fix
Enterprise License Manager 9.1(1) does not recognize Cisco Unified Communications Manager 9.0(1)	Enterprise License Manager 9.1(1) does not recognize Cisco Unified Communications Manager 9.0(1) license requirements.	Upgrade Cisco Unified Communications Manager Release 9.0(1) to 9.1(1). If your license file includes UWL Premium or Advanced UCL, contact Cisco at uc91-license@cisco.com for license file replacement.

Open Caveats for IM and Presence Release 9.0(1)

The following table lists open caveats which may cause unexpected behavior in IM and Presence 9.0(1).

Table 6: Open Caveats for IM and Presence

Identifier	Severity	Component	Headline
CSCua93235	3	database	EPE does not automatically remove NONE roster entry when state transition is FROM to NONE.
CSCua12285	3	database	Boot up after switch back hanging at 'Starting cupOnL2BootInitd'
CSCua41574	3	epe	HA issue: users logging out on the sub when xcp router comes up on pub
CSCua09500	3	epe	Presence engine hangs on startup.
CSCtz96324	3	gui	Auditor user does not have exclusive permission to audit log files.
CSCtz50782	3	gui-admin	Incorrect CUCM Hostname can cause Subscriber Install to fail.
CSCua09925	3	intercluster	ICSA peer has null remoteid causing SQLException in logs
CSCua20808	3	licensing	CLI incorrectly warns that a new license is required upon parameters change.
CSCua63152	3	security	Login failure after converting LDAP Synchronized User to Local User
CSCtz25566	3	security	HA can't be enabled - version missing
CSCua09717	3	security	DRF fails to backup Subscriber node.



CHAPTER 7

Documentation Updates

- License Mac References, page 50
- Administration Guide, page 50
- Bulk Administration Guide, page 57
- Call Detail Records Administration Guide, page 58
- Changing IP Address and Hostname, page 65
- Command Line Interface Reference Guide, page 66
- Deployment Guide for IM and Presence Service, page 67
- Dialed Number Analyzer Guide, page 68
- Disaster Recovery System Guide, page 68
- Features and Services Guide, page 69
- Installing Cisco Unified Communications Manager, page 83
- Interdomain Federation for IM and Presence Service, page 85
- Managed Services Guide, page 86
- Online Help, page 87
- OS Administration Guide, page 89
- Partitioned Intradomain Federation for IM and Presence Service, page 91
- Real-Time Monitoring Tool Guide, page 91
- Security Guide, page 94
- Serviceability Guide, page 100
- SIP Transparency and Normalization Developers Guide, page 103
- System Guide, page 103
- TCP and UDP Port Usage Guide, page 107
- Upgrade Guide, page 108
- User Options Guide, page 109

- XML Developers Guide, page 110
- Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service, page 110
- Online Help for Cisco Unified Communications Manager, page 111
- Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager, page 112

License Mac References

This documentation update resolves CSCul10528.

In Unified Communications Manager 9.x and later, the license mac is no longer used for licensing purposes; Enterprise License Manager handles licensing. Please ignore references to the license mac in the documentation.

Administration Guide

Access Control Group Permissions Interactions

This documentation update resolves CSCud59343.

Users can belong to multiple access control groups. When adding a new access control group to existing users, an unexpected reduction in the current level of privileges for some preexisting access control groups may be experienced if the new access control group has the “Effective Access Privileges for Overlapping User Groups and Roles” Enterprise parameter set to Minimum.

Access privilege reduction can occur inadvertently, for example, during an upgrade of Cisco Unified Communications Manager Administration. If the upgrade version supports the Standard RealTimeAndTrace Collection user group, which has the “Effective Access Privileges for Overlapping User Groups and Roles” Enterprise parameter set to Minimum, all users are automatically added to that user group during the upgrade. To resolve the permissions issue in this example, you can remove users from the Standard RealTimeAndTrace Collection user group.

Application User AXL Password Must Not Contain Special Characters

This documentation update resolves CSCud34740.

The following note is missing from the Application User Settings chapter in the *Cisco Unified Communications Manager Administration Guide*:

Note Do not use special characters when you cwreate an AXL password for an application user.

BFCP is Supported with TelePresence MCU

This documentation update resolves CSCuh70981.

The section "Conference Bridge Types in Cisco Unified Communications Manager Administration" incorrectly states that Binary Floor Control Protocol (BFCP) is not supported between Cisco Unified Communications Manager and a Cisco TelePresence Multipoint Control Units (MCU).

The system supports presentation sharing with the BFCP between Unified Communications Manager and a TelePresence MCU.

Convert LDAP Synchronized User to Local User Check Box Field Description Is Missing

The End User configuration window contains a check box that allows you to convert an LDAP synchronized user to a local user. The description for this check box is missing from the *Cisco Unified Communications Manager Administration Guide*, as well as this troubleshooting information:

When an LDAP synchronized user is converted to a local user within a system enabled for LDAP authentication, after the conversion process completes, users experience sign-in failures from:

- Cisco Unified CM IM and Presence Administration
- Cisco Unified IM and Presence Serviceability Administration
- Cisco Unified Personal Communicator
- Cisco Jabber
- Third Party XMPP Clients
- All externally supported interface that requires user authentication (except PAWS API)

To resolve the sign-in problem, perform one of these actions:

- Perform a manual synchronization from the **System** > **LDAP** > **LDAP Directory** menu. See “LDAP directory setup” in the *Cisco Unified Communications Manager Administration Guide*.
- Resolve the problem during a scheduled synchronisation.

See “LDAP directory setup” in the *Cisco Unified Communications Manager Administration Guide*.

Connected Lined ID Presentation Value

This documentation update resolves CSCug28060.

Descriptions of the Connected Line ID Presentation parameter were updated to include the following statement:

If a call that originates from an IP phone on Cisco Unified Communications Manager encounters a device, such as a trunk, gateway, or route pattern, that has the Connected Line ID Presentation set to Default, the presentation value is automatically set to Allowed.

Call Stats Field Removed

This documentation update resolves CSCug63874.

On the **Device** > **Device Settings** > **SIP Profile** setup window, the **Call Stats** option has been removed.

Common Phone Profile Settings Secure Shell Information

This documentation update resolves CSCug58742.

In the Common phone profile settings, the Secure Shell Password field is incorrectly referred to as the Secure Shell User.

Default Device Pool May Not Be Chosen After Upgrades to 5.x or Later

This documentation update resolves CSCtw79487.

If you upgrade an existing system to 5.x or later and your system includes new device types, the Default Device Pool may not be selected for the new device types. After the upgrade, you must check to ensure that the Device Pool that you want is assigned.

Device Mobility Calling Search Space is Used When Device CSS is set to None

This documentation update resolves CSCuc79185.

The following note is missing from "Phone Settings" in the *Cisco Unified Communications Manager Administration Guide*:

Note When set to <none>, Unified CM uses the device mobility calling search space, which is configured on the device pool.

End User Settings Correction

This documentation update resolves CSCue51184.

In the End User Configuration window, the Primary User Device field content has been removed.

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.

An ILS Restart is Required for Changes to Directory URI Catalogs

This documentation update resolves CSCur52619.

The following note is omitted from the "Intercluster Directory URI" chapter in the *Administration Guide* for Unified Communications Manager, Release 9.x:

Note When ILS is configured and a route string is changed on an Imported Directory URI Catalog, a restart is required so that the hub can update this catalog and remove old cached entries when making a call with an ILS lookup.

The restart is only to update the hub and not the spoke clusters. The spoke clusters receive the update within the synchronization cluster time that is configured on the **ILS Configuration** window.

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.

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.

Link Loss Type Field is Relabeled

This documentation update resolves CSCue58074.

On the **System** > **Region** configuration window, the Link Loss Type field has been relabeled as the Audio Codec Preference List field.

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 Exceptions for Voicemail Pilot

This documentation update resolves CSCtw44980.

The following information is missing for the Voice Mail Pilot Name field description in "Voice-Mail Pilot Settings" in the *Cisco Unified Communications Manager Administration Guide*:

Allowed characters are numeric (0-9), plus (+), asterisk (*), and pound (#).

Missing Tip for Naming a Server

This documentation update resolves CSCuc10415.

The following tip is missing from the "Server settings" topic in the *Cisco Unified Communications Manager Administration Guide*.

Tip To avoid errors, we recommend that you add a server to the system with a name that has less than 47 characters. Then, update the server name to the target length.

Option For Voicemail Usage Description

This documentation update resolves CSCtw44786.

The following description about For voice mail usage option has been added to the Add hunt list procedure in step 6.

"If you check the For Voice Mail Usage check box, the route list control process keeps a count of the setups that are being served to the hunt list, and will not allow more setups than the number of available devices. As a result, each device in the hunt list is treated as if it has a Busy Trigger and related Maximum Number of Calls of one".

"For example, if the hunt list contains five devices, and if busy trigger is two for each member, with the For Voice Mail Usage checkbox unchecked, it can process up to ten setups. For the same number of hunt list devices with a busy trigger of two for each member, with the For Voice Mail Usage checkbox checked, it can process only five setups and the next immediate setup after five gets rejected".

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.

Route Class Configuration SIP Information

This documentation update resolves CSCub65671.

If the route pattern points to a SIP trunk supporting G.Clear, then specify Data or Hotline as the Route Class.

You can use non-default route class settings to translate an inbound T1 CAS route class digit into a Cisco Unified Communications Manager route class value (and strip off the digit). You should not need to assign a non-default route class setting to any other inbound calls that use pattern configuration.

Service Name Cannot Be Localized

This documentation update resolves CSCuh62299.

The following note is added to the Service Name field under IP phone service settings table in the *Cisco Unified Communications Manager Administration Guide*.

Note When the service URL points to an external customized URL, you cannot localize the service name as per the device locale of the phone. The service name gets displayed in English alphabets only.

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.

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.

Use Personal Preference Field is Relabeled

This documentation update resolves CSCug52147.

On the **Call Routing** > **Route/Hunt** > **Hunt Pilot** setup window, the **Use Personal Preferences** option has been renamed to **Use Forward Settings of Line Group Member**.

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.

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.

Bulk Administration Guide

Cannot Disassociate Devices from End Users Using BAT

This documentation update resolves CSCuc30279.

The Bulk Administration Tool (BAT) cannot be used to disassociate devices that are already associated to an end user.

If you manually delete a controlled device from an exported end-user record and then insert the modified user record back in to the Cisco Unified Communications Manager database as a custom CSV data file, the insertion appears successful when you check the job results using **Bulk Administration** > **Job Scheduler**. However, the controlled device is still listed on the End User Configuration window in Cisco Unified Communications Manager Administration.

FindAndList Gateway Template Does Not Display the Templates

This documentation update resolves CSCtj43528.

FindAndList Gateway Template does not display templates with less than five characters. To display the list of templates, create a template with more than five characters.

Missing Note in Insert Phone Topic

This documentation update resolves CSCug41922.

The following note is missing from "Insert Phones in to Cisco Unified Communications Manager":

Note BAT expects Directory Number URI fields for directory numbers in the following format:

URI 1 on Directory Number 1, URI 1 Route Partition on Directory Number 1, URI 1 is Primary on Directory Number 1.

Model Is Not a Valid Device Field When Generating Phone Reports

This documentation update resolves CSCui06050.

"Phone and IP telephony device reports" lists Model as a device field. However, this field is not an option in the Bulk Administration Tool.

Call Detail Records Administration Guide

Call Recording Samples in CDR Examples Chapter

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

Field Names	Recorded Call CDR	Recording Call CDR1	Recording Call CDR2
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

Field Names	Recorded Call CDR	Recording Call CDR 1	Recording Call CDR 2
dest_CauseValue	0	0	0
origCalledPartyRedirectReason	0	354	354
lastRedirectRedirectOnBehalfOf	0	354	354
origCalledPartyRedirectOnBehalfOf		27	27
lastRedirectRedirectOnBehalfOf		27	27
origConversationID	0	16777113	16777113

Change Order of HuntPilotDN

This documentation update resolves CSCul25436.

The following attributes order is incorrect in *Cisco Unified Communications Manager Call Detail Records Administration Guide*

The documented order for HuntPilotDN and HuntPilotPartition should be reversed to HuntPilotPartition and HuntPilotDN

FinalCalledPartyNumber Field Description Is Incorrect

This documentation update resolves CSCub12688.

The Cisco Unified Communications Manager Call Detail Records Administration Guide states that the FinalCalledPartyNumber record represents a numeric string of up to 48 characters that can be either digits or a SIP URL. This information is incorrect. The field does not have a 48 character limit and can be an alphanumeric string that can be either digits or a SIP URL.

Missing CDR Field Descriptions

This documentation update resolves CSCud20005.

The following field descriptions are omitted from the *Cisco Unified Communications Manager Call Detail Records Administration Guide*:

wasCallQueued

This field specifies whether the call has been put into a queue. A value of 0 means that the call is not put into any queue; 1 means the call has been put into a queue.

totalWaitTimeInQueue

This field specifies how long a caller has been in a queue. The value is specified in seconds. The value is 0 if the call was never put into any queue.

Missing CDR Field Descriptions for IMS Application Server

This documentation update resolves CSCum60891.

The following CDR field descriptions in the table below for IMS Application Server are omitted from the *Call Detail Records Administration Guide*.

Field Name	Range of Values	Description
incomingICID	Text String	Alphanumeric string up to 50 characters This field is populated with the IMS Identifier(ICID) from the P-Charging Vector at the incoming call leg of the call. This field will be empty when the call leg has no IMS or SIP trunk with P-Charging-Vector enabled. Default = Empty String " "
incomingOrigIOI	Text String	Alphanumeric string up to 50 characters This field is populated with the originating Interoperator Identifier(IOI) from the P-Charging Vector at the incoming call leg of the call. This field will be empty when the call leg has no IMS or SIP trunk with P-Charging-Vector enabled. Default = Empty String " "
incomingTermIOI	Text String	Alphanumeric string up to 50 characters This field is populated with the terminating Interoperator Identifier(IOI) from the P-Charging Vector at the incoming call leg of the call. This field will be empty when the call leg has no IMS or SIP trunk with P-Charging-Vector enabled. Default = Empty String " "
outgoingICID	Text String	Alphanumeric string up to 50 characters This field is populated with the IMS Identifier(ICID) from the P-Charging Vector at the outgoing call leg of the call. This field will be empty when the call leg has no IMS or SIP trunk with P-Charging-Vector enabled. Default = Empty String " "

Field Name	Range of Values	Description
outgoingOrigIOI	Text String	Alphanumeric string up to 50 characters This field is populated with the originating Interoperator Identifier(IOI) from the P-Charging Vector at the outgoing call leg of the call. This field will be empty when the call leg has no IMS or SIP trunk with P-Charging-Vector enabled. Default = Empty String " "
outgoingTermIOI	Text String	Alphanumeric string up to 50 characters This field is populated with the terminating Interoperator Identifier(IOI) from the P-Charging Vector at the outgoing call leg of the call. This field will be empty when the call leg has no IMS or SIP trunk with P-Charging-Vector enabled. Default = Empty String " "
outpulsedOriginalCalledPartyNumber	Text String	Alphanumeric string up to 50 characters The Original called party number outpulsed from the device. Default = Empty String " "
outpulsedLastRedirectingNumber	Text String	Alphanumeric string up to 50 characters The Last Redirecting number outpulsed from the device. Default = Empty String " "

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

Change the Hostname Using the Unified Communications Operation System Administration GUI

In the procedure "Change hostname using Unified Communications Operation System Administration GUI," there is an error in the output displayed for step 5, which directs you to use the **utils network host** command to verify that the name-IP association has propagated to other nodes. When you use the command, the output should read as follows:

```
admin:utils network host sub-4
Hostname sub-4 resolves to 198.50.103.11
```

Missing Step in Unified CM Hostname Update

This documentation update resolves CSCub59376.

There is a missing step in each of the procedures that describe how to change a server hostname in the *Changing the IP Address and Hostname for Cisco Unified Communications Manager* document. Immediately after you change the hostname of a Unified CM server and save your changes, the server reboots automatically. Immediately after the server reboots, you must bring up the Admin CLI for the server on which the hostname was changed and run the **utils dbreplication dropadmin db** command. This step applies to any procedure that involves a hostname change for Cisco Unified Communications Manager.

Command Line Interface Reference Guide

The following CLI commands were added to the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*, Release 9.0(1):

- utils ntp server add
- utils ntp server delete

To view the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* for your release, see the below URL.

CSCum43072 run cuc sysagent task Example Incorrect

The example for the command **run cuc sysagent task** is incorrect. The command line should state the following: run cuc sysagent task Umss.CleanDeletedMessagesTask.

The following content is missing: For a list of Sysagent tasks, run the command show cuc sysagent task list (Cisco Unity Connection Only). Be aware that sysagent task names are case sensitive.

CSCuo56537 Enable Disable FIPS for IM and Presence Service

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 Servicee subscriber node cannot access information from the IM and Presence Service database publisher node. For example, a user who is logged into the Cisco Unified Serviceability GUI on a subscriber node will not be able to view services on theIM and Presence Service database publisher node. Users will see the following error message until the sync is complete: `Connection to server cannot be established (certificate exception)`

CSCup03425- CUCM 9.1 CLI guide has conflicting information for "set network domain"

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

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.

Related Topics

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

ILS Troubleshooting Tips Corrections

This documentation update resolves CSCun09203.

The following information applies to the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

utils ils show peer info should be **utils ils showpeerinfo**.

utils ils find route is an invalid command.

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.

Trace Option for Show Media Streams CLI Command

This documentation update resolves CSCtt41576.

The trace option for the **show media streams** cli command activates extra trace from the media driver to the system log.

Note Ignore any kernel messages that display on the console screen when **show media streams trace** is entered.

Deployment Guide for IM and Presence Service

Exceeding Maximum Contact List Settings During Contact List Import Is Supported

This documentation update resolves CSCug87105.

It is possible to exceed the maximum contact list size setting without losing data when importing user contact lists to IM and Presence Service using BAT; however, Cisco recommends temporarily increasing the Maximum Contact List Size setting or setting the value to Unlimited for the import. You can reset the maximum value after the import is complete.

Legacy Clients

When initially configuring your system for Cisco clients, use **Cisco Unified CM IM and Presence Administration** > **Application** > **Legacy Clients** to configure the settings below:

- Proxy Listener
- TFTP Servers
- LDAP Client Attribute Mapping
- Cisco CallManager Cisco IP Phone (CCMCIP) service

Note In future releases of Jabber clients, some of these settings may no longer need to be configured.

For information about setting these values, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager, Release 9.0(1)*: http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_configure.html.

Dialed Number Analyzer Guide

Find and List Phones in DNA Using Directory URI

This documentation update resolves CSCuc55921.

Dialed Number Analyzer (DNA) provides a Phones window where you can find and list phones by device name, description, directory number, Directory URI, calling search space device pool, device type, and call pickup group. You can find a phone and choose it as a calling device for the analysis that you want to perform. You can further choose a configured phone line (directory number) and use it as a calling party number.

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 7: SFTP Server Information

SFTP Server	Information
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.

System Backup File Encryption

This documentation update resolves CSCui75485.

A note was added to the topic describing how to view the backup history, which clarifies that the Cisco Unified Communications Manager and IM and Presence Service backup job files are encrypted and can be opened only by the system software.

Updated Caution to Include DNS and Domain Name Prior To Restore

This documentation update resolves CSCul28047.

The following caution is updated to include DNS and domain name prior to performing a restore:

Caution Before you restore Cisco Unified Communications Manager, ensure that the hostname, IP address, DNS configuration, domain name, version, and deployment type of the restore matches the hostname, IP address, DNS configuration, domain name, version, and deployment type of the backup file that you want to restore.

Features and Services Guide

Answer Too Late Timer

This documentation update resolves CSCtr78911.

In Cisco Unified Communications Manager Administration, use the **Device** > **Remote Destination** menu path to configure remote destinations.

Answer Too Late Timer

Enter the maximum time in milliseconds that Cisco Unified Communications Manager allows for the mobile phone to answer. If this value is reached, Cisco Unified Communications Manager stops ringing the mobile phone and pulls the call back to the enterprise.

Range: 0 and 10,000 - 300,000 milliseconds

Default: 19,000 milliseconds

If the value is set to zero, the timer is not started.

Call Mobility Missing Information

The following limitation is missing from the "Cisco Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*:

Cisco Unified Communications Manager does not support Unified Mobility with Call Queuing.

Call Park Display Timer Restriction

This documentation update resolves CSCug36365.

The interaction between the value that is entered for the Call Park Reversion Timer and the Cisco Call Park Display Timer must be updated in the Call Park restrictions section as follows:

If you entered a Call Park Reversion Timer value that is less than the Call Park Display Timer, Call Park numbers may not display on the phone.

Call Pickup Phones Supported

This documentation update resolves CSCue92900.

The following information is omitted from the table that lists phones that support Call Pickup:

The Cisco Unified IP Phone series 7900, 8900, and 9900 support both softkey and button activated Call Pickup. For the 3500 Cisco Unified IP Phone, the Call Pickup feature is activated using the menu.

Call Queuing Interaction with Hunt Groups and Hunt Pilots

This documentation update resolves CSCue08776.

The logoff notification functionality for hunt groups changes when Call Queuing is enabled for a hunt pilot. The Hunt Group Logoff Notification does not play when a user logs out of a hunt group, or is logged off because they missed their turn in the queue, if Call Queuing is enabled for a hunt pilot.

Call Queuing Missing Information

The following limitation is missing from the "Call Queuing" chapter in the *Cisco Unified Communications Manager Features and Services Guide*:

Cisco Unified Communications Manager does not support Unified Mobility with Call Queuing.

Call Queuing Not Supported with Mobile Device Types

Cisco Unified Communications Manager does not support Call Queuing with mobile device types.

Call Queuing Shared Line Scenario Description

This documentation update resolves CSCue98877.

In the Call queuing operation considerations section, the paragraph describing shared-line deployments should read as follows:

For shared-line deployments, the availability of all devices with that shared-line are combined to provide a final status. If a shared-line device for one or members appears as on-hook, but all others are indicating off-hook, the final status for that line member remains off-hook.

Call Waiting Behavior with MLPP Preemption Correction

This documentation update resolves CSCub10861.

When a Routine precedence call is offered to a destination station that already has active calls that are configured with call waiting, normal call waiting is activated if the existing call count is less than the busy trigger.

When a non-routine precedence call is offered to a destination station that already has an active call that is configured with call waiting, precedence call waiting is activated if the existing call count is less than the busy trigger and any of the following conditions exist:

- The device supports visual call appearances and has an open appearance.
- The device supports two non-visual call appearances and has an open appearance, and the precedence of the new call is equal to or lower than the existing call.
- The device has an open appearance (visual or non-visual) and the device is non-preemptable.

When a non-routine precedence call is offered to a destination station that already has an active call that is configured with call waiting, an existing lower-precedence call is preempted if the existing call count is equal to or greater than the busy trigger.

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.

Centralized Proxy TFTP File Signature Verification Failure

This documentation update resolves CSCud18710.

When a phone requests a common file from a central or proxy TFTP server and that file has a common name such as `ringlist.xml.sgn` or is a locale file, the TFTP server sends its own local copy of the file instead of the file from the home cluster of the phone. The phone rejects the file due to a signature verification failure because the file has the signature of the TFTP server's local cluster, which does not match the Initial Trust List (ITL) of the phone. To resolve this issue, you can either disable Security By Default (SBD) for the phone or perform the bulk certificate export procedure to make the Trust Verification System (TVS) return a success when the phone verifies a signature from a different cluster. See the procedure in the "Default Security Setup" section of the *Cisco Unified Communications Manager Security Guide* for performing a bulk certificate export when migrating IP phones between clusters. To disable Security by Default, see the procedure to update the ITL file for IP Phones in the *Cisco Unified Communications Manager Security Guide*.

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, 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.

Configuring OpenAM Section

This documentation update resolves CSCup44177.

The following content is missing from the "Configure OpenAM" section of "Single Sign-On" chapter:

After you install the OpenAM server, you must ensure that a default account is created so that you can enable and configure the SSO-based authentication successfully on Cisco Unified Communications Manager applications. The default account consists of a “demo” username and a password. To enable Agent Flow SSO on Unified Communications applications, the system uses this default account to validate the following that are provisioned on OpenAM:

- Login module
- J2EE agent

To verify if the “demo” user is configured or not, perform the following procedure:

Procedure

Step 1 Log in to the OpenAM server.
The OpenAM administration window appears.

Step 2 Select the **Access Control** tab.
A list of one or more access control realms appears.

Step 3 Click **Top Level Realm**.

Note The top level realm appears in the list when you deploy the OpenAM server. This realm contains the OpenAM configuration data.

An additional set of configuration tabs appears.

Step 4 Select the **Subjects** tab.

Step 5 Click **New**.
A list of fields containing user details appears.

Step 6 Enter data for the following fields:

- **ID**: demo
- **First Name**: demo
- **Last Name**: demo
- **Full Name**: demo
- **Password**: changeit
- **Password (confirm)**: changeit

  Note Do not change this default password.

- **User Status**: Select the **Active** radio button.

Step 7 Click **OK**.
The system creates a “demo” user successfully.

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.

Corrections for the Immediate Divert Feature

This documentation update resolves CSCun20448.

Steps 6 and 7 are incorrect for the “Configure Immediate Divert” procedure in the *Features and Services Guide*. The following are the corrected steps.

Configure Immediate Divert

Step 6

Standard User or Standard Feature softkey is copied to a new template and then the template is used to assign iDivert softkey. Assign the softkey in the Connected, On Hold, and Ring In states. Divert softkey in Cisco Unified IP Phones 8900 series gets enabled using the softkey template and for the 9900 series the Divsert softkey feature gets enabled using feature control policy template.

Step 7

In the Phone Configuration window, assign the newly configured softkey template which has iDivert enabled, to each device that has immediate divert access.

System requirements for Immediate Divert

The following table lists the phones that use the Divert or iDivert softkey. The 8900 and 9900 series contain system requirement changes:

- Cisco Unified Communications Manager 6.0 or later
- ***Table 8: Cisco Unified IP Phones That Use iDivert or Divert Softkeys***

Cisco Unified IP Phone Model	Divert Softkey	iDivert Softkey	What to configure in softkey template
Cisco Unified IP Phone 6900 Series (except 6901 and 6911)	X		iDivert
Cisco Unified IP Phone 7900 Series		X	iDivert
Cisco Unified IP Phone 8900 Series	X		iDivert
Cisco Unified IP Phone 9900 Series	X		iDivert

Early Media Cut-Through and Single Number Reach Missing Information

The following information is omitted from the "Cisco Unified Mobility" chapter in the *Cisco Unified Communications Manager Features and Services Guide*:

Early Media cut-through is not supported for Single Number Reach (SNR) calls. SNR follows shared line behavior and does not function as desired with early media cut-through.

For example, Phone A (DN 1000) calls Phone B (DN 1001) which has an Remote Destination Phone C(DN 1001), sharing line with Phone B . When you enable early media cut-through and place a call to Phone B, both shared lines do not ring, because with early media cut-through enabled, a device may signal a connect, causing the other device to stop ringing.

To avoid this behavior, do not configure early media cut through on the outbound trunk or gateway for SNR.

EMCC Logout Limitation

This documentation update resolves CSCue04792.

In the visiting cluster, the current Phone Configuration window has a Log Out button for intracluster Extension Mobility (EM). This button is also used by the visiting cluster administrator to log out an Extension Mobility Cross Cluster (EMCC) phone. Because the EMCC phone is not currently registered with the visiting Cisco Unified Communications Manager, this operation is equivalent to a database cleanup in the visiting cluster. The EMCC phone will remain registered with the home Cisco Unified Communications Manager until it comes back to the visiting cluster due to a reset or a logout from the home cluster by other means.

EMCC Remote Cluster Menu

This documentation update resolves CSCue33160.

In the chapter Extension Mobility Cross cluster, step 20 of Configure EMCC, **Advance Features** > **EMCC** > **EMCC Remote Cluster** menu item should be **Advance Features** > **Cluster View**.

Empty Far-End When Recording Call Park for Some Phones

This documentation update resolves CSCud03278.

In the current Call Park implementation, the far-end or X-Refci may be empty when recording Call Park for phone models such as 997X, 995X and 896X.

Enable Mobile Connect for IP Multimedia Subsystem

This documentation update resolves CSCtz29138.

For IP Multimedia Subsystem, ensure that the Mobile Connect feature is enabled in the Remote Destination Configuration window, or by using one of the other methods prescribed for enabling Mobile Connect, before implementing Intelligent Session Control call processing.

Enterprise Feature Access and User Control

This documentation update resolves CSCui24499.

The following note is omitted from the Remote Destination settings table for the Single Number Reach Voicemail Policy field:

Note For User Control to work, you must set the Enable Enterprise Feature Access service parameter to TRUE.

Expansion Module Field Missing From Certain Device Profiles

This documentation update resolves CSCuc39511.

The expansion module field is not listed on the Device Profile Configuration window for Cisco Unified IP Phone models 8961, 9951, and 9971. No manual selection is required. The lines from the Phone Button Template are applied to the physical device no matter which expansion modules these phones use.

Skip step 9 in the procedure to "Create the device profile for a user" as documented for Cisco Extension Mobility configuration in the *Cisco Unified Communications Manager Features and Services Guide*.

Step..**9**	If the phone type supports Cisco Unified IP Phone Expansion Modules, Cisco Unified Communications Manager displays expansion module field. At the Module 1 drop-down list box and at the Module 2 drop-down list box, choose the appropriate expansion module.

Extension Mobility Equivalency Changes

This documentation update resolve CSCuh56102.

The following information is omitted from the "Extension Mobility Equivalency" section:

- All mentions of Feature Safe and Feature Safe Configuration are removed.
- Added a new section "EM Equivalency during login" which mentions:

  Size safe phones use the template from the login profile and the template is applied as described in "Size Safe Feature" section. Non-size safe phones must use the template that is associated with the default device profile for the model and protocol that matches the phone that the user logs into.

  Note The device that the user logs into must support Size Safe on Phone Template for EM Equivalency. The capability of the EM Profile does not effect EM Equivalency during login.

- Modified the below paragraph and listed the supported SCCP and SIP phones for EM Equivalency

  Cisco Unified Communications Manager enhances the existing Extension Mobility (EM) equivalency mechanism to work across both SCCP and SIP protocols on the following models:

  - Cisco 7906

- Cisco 7941
- Cisco 7941G-GE
- Cisco 7942
- Cisco 7945
- Cisco 7961
- Cisco 7961G-GE
- Cisco 7962
- Cisco 7965
- Cisco 7970
- Cisco 7971
- Cisco 7975
- Cisco IP Communicator

Extension Mobility Missing Information

The following information is missing from the “Cisco Extension Mobility” chapter.

The following table lists caveats and workarounds for using Cisco Extension Mobility during a node upgrade.

Table 9: Cisco Extension Mobility Behavior During Node Upgrade

Caveat	Workaround
When you perform an upgrade on the EM service node, the upgrade process increases the CPU load percentage. The CPU used during upgrade of the EM service node can increase to 80% and higher. **Caution** Some EM logins may fail because of high CPU use threshold during an upgrade.	• Sign in to another EM node to shift the CPU load from the upgraded node to another node. • Create another EM service that goes to another node that you are upgrading.

Caveat	Workaround
When the EM service node finishes upgrade and then reboots, users cannot sign in or sign out using the EM service. However, they can sign in or sign out if they configured another EM service that points to another active node. If the phone performs a failover to a node on the old database, the user can still successfully sign in to and sign out of EM. But when the phone performs failback to the newly upgraded node that connects to the new database, the updates that occurred during the failover to the old database node do not appear on the phone until the failover node is successfully upgraded to the new version. In the meantime, the user needs to sign in or sign out of EM against the newly upgraded failback node.	None.
After you upgrade the TFTP node, it reboots and goes offline. If you sign in using EM and the EM service is not configured with TFTP and has a separate node, it signs in but does not load the new EM configuration to the phone.	Create an alternative TFTP that loads the EM configuration from another node onto the phone.

Hunt Pilots Limit for a Call Queue

This documentation update resolves CSCuj75419.

The following note is missing from the Call Queuing operation section:

Note You can configure a maximum of 25 hunt pilots per hunt list in Call Queuing. If you exceed this limit, the queue status will not be displayed.

iDivert Feature Correction

The *Cisco Unified Communications Features and Services Guide* states that the iDivert feature does not work in cases where the redirect signal must traverse a QSIG link. This statement is incorrect. The statement should read that the iDivert feature does not work in cases where the feature has been initiated via CTI and the redirect signal must traverse a QSIG link.

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.

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.

MLPP Parameters

In Cisco Unified Communications Manager Administration, you can use the**Device** > **Phone** menu to configure the following MLPP parameters:

- MLPP Domain
- MLPP Preemption
- MLPP Indication

If you do not set the MLPP parameters on the **Phone Configuration** window, the system uses the settings configured in the common device configuration. If the MLPP paramaters are not configured in the common device configuration, then the settings from the enterprise parameters are used. MLPP parameters are not inherited from settings in the device pool.

New Audio Files for Music On Hold

This documentation update resolves CSCut93896.

The following information is omitted from the "Music On Hold" chapter in the *Features and Services Guide*.

Problem When you upload an audio file with the same name as an existing file that is mapped to an Audio Source ID, your users may hear the existing file still playing back.

Solution To ensure that the updated file is played, follow these steps:

1. After you upload the new audio file to replace the old one, find the audio source ID you want to change under the **Music On Hold Audio Source Configuration** window.
2. Select a different audio source file, such as the default **SampleAudioSource** and then click **Save**.
3. Switch the source file back to your file you want to use, and then click **Save**.
4. Reset the Music On Hold server so that the changes take effect.

No Audio After Pressing Mobility Button

This documentation update resolves CSCub51519.

In Unified CM 9.0(1), the Cisco Unified Mobile Communicator must be enabled for a mobile phone on the **Mobility Identity Configuration** window.

Play Continuously and Music On Hold

This documentation update resolves CSCue85258.

A reference to play continuously is listed in the Music On Hold audio source configuration settings table, but should be removed.

Queue Status PLK Supported Phone Models

This documentation update resolves CSCuc63315.

Queue status PLK is only supported with the following LCD display phones for both SCCP and SIP protocols:

- 6921
- 6941
- 6945
- 6961
- 7911 G
- 7931 G
- 7942 G
- 7945 G
- 7962 G
- 7965 G
- 7975 G
- 8961
- 8945
- 8941
- 9951
- 9971

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.

Remote Destination Single Number Reach and Enterprise Number Call Reroute

This documentation update resolves CSCts83374.

In Cisco Unified Communications Manager Administration, use the **Device** > **Remote Destination** menu path to configure remote destinations.

Single Number Reach

You can configure all of the Remote Destination Configuration Settings for Single Number Reach.

Reroute Remote Destination Calls to Enterprise Number

For the Reroute Remote Destination Calls to Enterprise Number, you can configure:

- Answer Too Soon Timer
- Answer Too Late Timer

For the Reroute Remote Destination Calls to Enterprise Number, you can not configure:

- Delay Before Ringing Timer
- Enable Mobile Connect
- Ring Schedule

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.

Secure Shell Password Maximum Length

The maximum length of a secure shell password is 50 characters. It can include any alphanumeric or special characters.

SIP Phones Support CMC and FAC Tones

This documentation update resolves CSCue33154.

The following bullet in the interactions and restrictions section of the Client matter codes and forced authorization codes chapter should be updated to include SIP:

- The FAC and CMC tones play only on Cisco Unified IP Phones that are running SCCP or SIP, TAPI/JTAPI ports, and MGCP FXS ports.

Support for Midcall Mobility Features with Cisco Unified Border Element

This documentation update resolves CSCua75983

Cisco Unified Mobility supports the Mobile Connect feature without mid-call features over SIP trunks with Cisco Unified Border Element (CUBE). To enable mid-call features, you must also configure an Enterprise Feature Access directory number and check the **Send send-receive SDP in mid-call INVITE** check box that appears in the SIP Profile Configuration window of the SIP profile that is assigned to the SIP trunk.

User Control System Parameters Correction

The *Cisco Unified Communications Features and Services Guide* states that the value you specify for the **User Control Delayed Announcement Timer** and **User Control Confirmed Answer Indication Timer** parameters is in seconds. This statement is incorrect. The value for these parameters is in milliseconds.

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.

4000 Series Integrated Services Routers do not support Mobile Voice Access

This documentation update resolves CSCvb33454.

The following limitation has been omitted from the *Cisco Unified Mobility* chapter of the *Feature and Services Guide*.

Mobile Voice Access (MVA)

Cisco 4000 Series Integrated Services Routers do not support Voice XML (VXML). Hence, when these routers function as Unified Communications gateways with Cisco Unified Communications Manager, they do not support Mobile Voice Access (MVA) application.

Installing Cisco Unified Communications Manager

Cisco Unified CM Installation on MCS 7825 H3 and 7828 H3 Server Models

This documentation update resolves CSCtr49649.

Note the following revision to step 5 of the Install software procedure in *Installing Cisco Unified Communications Manager, Release 9.0(1)*.

Step 5

The system installer performs the following hardware checks to ensure that your system is correctly configured. If the installer makes any changes to your hardware configuration settings, you will get prompted to restart your system. Leave the DVD in the drive during the reboot:

- First, the installation process checks for the correct drivers, and you may see the following warning:

```
No hard drives have been found. You probably need to manually choose
 device drivers for
install to succeed. Would you like to select drivers now?
```

  To continue the installation, choose **Yes.**

- The installation next checks to see whether you have a supported hardware platform. If your server does not meet the exact hardware requirements, the installation process fails with a critical error. If you think this is not correct, capture the error and report it Cisco support.
- The installation process next verifies RAID configuration and BIOS settings.

Note For MCS 7825 H3 and MCS 7828 H3 Server models, the installation process detects and disables the SATA RAID, if enabled. The **System Rebooting Intermediately** window appears with the message

System is going to reboot for SATA RAID to be disabled in BIOS Press any key to continue
This disables the SATA RAID and reboots the system. On reboot, the installation will continue and will activate the Linux SW RAID.

Note If this step repeats, choose **Yes** again.

- If the installation program must install a BIOS update, a notification appears telling you that the system must reboot. Press any key to continue with the installation.

After the hardware checks complete, the Product Deployment Selection window displays.

Disable ICH10 Onboard SATA Controller on EX/ESXi Servers During Unified CM Installation

This documentation update resolves CSCtk68384.

If the server is running VMware EX/ESXi and the motherboard has an ICH10 onboard SATA controller, you must disable the SATA controller in the BIOS. The ICH10 onboard SATA controller is not supported by EX/ESXi. Perform the following steps to disable the SATA controller in the BIOS as a pre-installation task when installing the Cisco Unified Communications Manager.

1. Boot the server and press F2 when prompted during boot up.
2. Select **Advanced** tab.
3. Select **Mass Storage Controllers Configuration**.
4. Set the Onboard SATA Controller to **Disabled**.

Installation Fails with Unrecoverable Internal Error

This documentation update resolves CSCug84842.

Application User Name and Password

When you install Cisco Unified Communications Manager, you must enter an Application User name and password. You use the Application User name and password to access applications that are installed on the system, including the following areas:

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Real Time Monitoring Tool
- Cisco Unified Reporting

To specify the Application User name and password, follow these guidelines:

- Application User name - The Application User name must start with an alphabetic character and can contain alphanumeric characters, hyphens and underscores.
- Application User password - The Application User password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

Caution Do not use the system application name as the Application User name. Using a system application name causes the installation to fail with an unrecoverable error during the installation of the database

System application names are:

- CCMSysUser
- WDSysUser
- CCMQRTSysUser
- IPMASysUser
- WDSecureSysUser
- CCMQRTSecureSysUser
- IPMASecureSysUser
- TabSyncSysUser
- CUCService

You can change the Application User name and password by using the command line interface. For more information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Post-Installation Tasks

Locales

When you install the Cisco Unified Communications Manager on a server, the locale English_United_States installs automatically; however you can add new locales to the server if required. If you add new locales, add them only after you have installed Cisco Unified Communications Manager on all servers in the cluster, and have set up the database.

COP Files

Install COP enabler files for any custom device types that you want to use that do not ship with Cisco Unified Communications Manager. Perform this task only after you have completed the installation for the entire cluster, and set up the database.

Interdomain Federation for IM and Presence Service

Cannot Install Signed Microsoft CA Server-Client Authentication Certificate on Microsoft OCS 2008

This documentation update resolves CSCtw47643.

You cannot install a server-client authentication certificate that is signed by a Microsoft certificate authority (CA) into the local computer store of a Microsoft Office Communications Server (OCS) running Windows

2008. Attempting to copy the certificate from the current user store to the local computer store fails with the error message that the private key is missing.

To resolve this issue, perform the following procedure:

1. Log on to the OCS as a local user.
2. Create the certificate.
3. Approve the certificate from the CA server.
4. While logged on to the OCS, export the certificate to a file and ensure that the private key is exported.
5. Log off the OCS (Local Computer).
6. Log on to the OCS again, but this time log on to the OCS domain as a domain user.
7. Use the Certificate Wizard to import the certificate file. The certificate is installed in the local computer store. You can now select the certificate in the OCS certificate tab.

FIPS Not a Requirement for Federated Connections with LYNC 2010 Servers

This documentation update resolves CSCui45519.

Federal Information Processing Standard (FIPS) is not required for federated connectivity over TLSv1 encrypted connections with Microsoft Lync 2010 servers. Content that was related to configuring FIPS for Lync servers have been removed from the guide.

Use TLS for Static Routes

This documentation update resolves CSCui01368.

You must use TLS for static routes with Microsoft Lync servers. The TCP option for static routes between Microsoft Lync servers and IM and Presence Service was removed and some sections restructured.

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

404 Errors in Unified CM CDR Analysis and Reporting Online Help

Some GUI menu items return broken links in the CDR Analysis and Reporting online help when you click **Help** > **For this page**.

The following table lists paths to GUI menu items with broken online help links and the workaround to access the online help.

Table 10: GUI Menu Items in CDR Analysis and Reporting

GUI path	Workaround
• **System Reports** > **QoS** > **Detail** • **System Reports** > **QoS** > **By Call Types**	1 Select **Help** > **Contents and Index**. 2 Navigate to **System reports** > **QoS system reports** in the left-hand pane.
• **Device Reports** > **Gateway** > **Detail** • **Device Reports** > **Gateway** > **Utilization**	1 Select **Help** > **Contents and Index**. 2 Navigate to **Device reports** > **Gateway device reports** in the left-hand pane.
• **Device Reports** > **Route Patterns/Hunt Pilots** > **Route and Line Group Utilization** • **Device Reports** > **Route Patterns/Hunt Pilots** > **Route/Hunt List Utilization** • **Device Reports** > **Route Patterns/Hunt Pilots** > **Route Pattern/Hunt Pilot Utilization**	1 Select **Help** > **Contents and Index**. 2 Navigate **Device reports** > **Route pattern and hunt pilot device reports** in the left-hand pane.
• **Device Reports** > **Trunk** > **Utilization**	1 Select **Help** > **Contents and Index**. 2 Navigate to **Device reports** > **Trunk device reports** in the left-hand pane.

GUI path	Workaround
• **System** > **Scheduler** > **Daily**	1 Select **Help** > **Contents and Index**. 2 Navigate to **System** > **CAR system scheduler** in the left-hand pane.
• **System** > **Database** > **Configure Automatic Purge**	1 Select **Help** > **Contents and Index**. 2 Navigate to **System** > **CAR system database** in the left-hand pane.
• **System** > **System Parameters** > **System Preference**	1 Select **Help** > **Contents and Index**. 2 Navigate to **System** > **CAR system parameters** in the left-hand pane.
• **Report Config** > **Rating Engine** > **Voice Quality**	1 Select **Help** > **Contents and Index**. 2 Navigate to **Report configuration** > **CAR rating engine** in the left-hand pane.

Update Users Documentation Does Not Appear in Context-Sensitive Help

From the Bulk Administration Tool, when you navigate to **Users** > **Update Users** > **Query** and click **Help** > **This Page**, the online help for this GUI menu item does not appear. The following workaround lets you access the documentation for this GUI menu item:

1 Click **Help** > **Contents**.

2 On the left-hand navigation menu, click **Cisco Unified Communications Manager Batch Administration** > **Users** > **User Updates** > **User Update Settings**

Device Name and Description Fields Need to Be Updated

In the Unified CM Administration menu **Device** > **Trunk**, the Device Name and Description fields should read as follows:

Device Name

Enter a unique identifier for the trunk. The device name can include up to 50 alphanumeric characters: A-Z, a-z, numbers, hyphens (-) and underscores (_) only.

Description

Enter a descriptive name for the trunk. The description can include up to 114 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

OS Administration Guide

ICSA Service Needs Restart After Ipsec Cert Is Regenerated

This documentation update resolves CSCul66341.

The following information was omitted from the IM and Presence Service Regenerate certificate topic.

If you regenerate an ipsec certificate, you must restart the Cisco Intercluster Sync Agent after you regenerate the certificate as follows:

- When you regenerate an ipsec certificate on the IM and Presence Service database publisher node, you must restart the Cisco Intercluster Sync Agent on the publisher node and then restart the Cisco Intercluster Sync Agent on all IM and Presence Service subscriber nodes in the cluster.
- When you regenerate an ipsec certificate on an IM and Presence Service subscriber node, you must restart the Cisco Intercluster Sync Agent service on that node, and then restart the Cisco Intercluster Sync Agent on all other nodes in the cluster.

Regenerate Certificate

This documentation update resolves CSCua63006 and CSCth80282.

You can regenerate certificates from the Cisco Unified Communications Operating System as an operating system security function. For more information about regenerating certificates, see the *Cisco Unified Communications Manager Security Guide*.

Caution Regenerating a certificate can affect your system operations. Regenerating a certificate overwrites the existing certificate including a third party signed certificate if one was uploaded.

Note Certificate regeneration or upload of a third party signed certificate should be performed during maintenance.

The following table describes the system security certificates you can regenerate from the Cisco Unified Communications Operating System and the related services that must be restarted. For information about regenerating the TFTP certificate, see the *Cisco Unified Communications Manager Security Guide*.

Table 11: Certificate Names and Descriptions

Name	Description	Related Services
tomcat	This self-signed root certificate is generated during installation for the HTTPS server.	tomcat
ipsec	This self-signed root certificate is generated during installation for IPsec connections with MGCP and H.323 gateways.	Cisco Disaster Recovery System (DRS) Local and Cisco DRF Master

Name	Description	Related Services
CallManager	This self-signed root certificate is installed automatically when you install Cisco Unified Communications Manager. This certificate provides server identification, including the server name and the Global Unique Identifier (GUID).	CallManager and CAPF
CAPF	The system copies this root certificate to your server or to all servers in the cluster after you complete the Cisco client configuration.	CallManager and CAPF
TVS	This is a self-signed root certificate.	TVS

If you regenerated the certificate for Cisco Certificate Authority Proxy Function (CAPF) or Cisco Unified Communications Manager and a CTL client is configured, rerun the CTL client.

After you regenerate certificates in the Cisco Unified Communications Operating System, you must perform a system backup so that the latest backup contains the regenerated certificates. If your backup does not contain the regenerated certificates and you perform a system restoration task, you must manually unlock each phone in your system so that the phone can register with Cisco Unified Communications Manager. For information about performing a backup, see the *Disaster Recovery System Administration Guide*.

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The Certificate List window displays.

Step 2 Click **Generate New**.
The Generate Certificate dialog box opens.

Step 3 Choose a certificate name from the Certificate Name list.
For details about certificate names, see the Certificate Names and Descriptions table.

Step 4 Click **Generate New**.
If intracluster communication is enabled using EMCC complete the following steps during certificate regeneration.

Step 5 Navigate to **Advanced Features > EMCC> Intercluster Service Profile** and deactivate **EMCC Service**.

Step 6 Logout all remotely logged in devices from **Device > Related Link > Remotely Logged In Device**.

Step 7 Regenerate certificates.

Step 8 Perform the Bulk Certification operation.

Step 9 Activate the **EMCC Service**.

What to Do Next

Restart all services that are affected by the regenerated certificate as listed in the Certificate Names and Descriptions table.

Rerun the CTL client (if configured) after you regenerate the CAPF or CallManager certificates.

Perform a system backup to capture the newly regenerated certificates. For information about performing a backup, see the *Disaster Recovery System Administration Guide*.

Partitioned Intradomain Federation for IM and Presence Service

Disable Empty TLS Fragments

This documentation update resolves CSCuh39611.

To support TLS encryption between IM and Presence Service and Microsoft Lync/OCS/LCS, you must modify the Peer Authentication TLS Context configuration on IM and Presence Service using the Cisco Unified CM IM and Presence Administration GUI. Ensure that you disable empty TLS fragments when you modify the Peer Authentication TLS Context on IM and Presence Service before integrating with Microsoft Lync/OCS/LCS for Partitioned Intradomain Federation.

FIPS Not a Requirement for Federated Connections with LYNC 2010 Servers

This documentation update resolves CSCui45519.

Federal Information Processing Standard (FIPS) is not required for federated connectivity over TLSv1 encrypted connections with Microsoft Lync 2010 servers. Content that was related to configuring FIPS for Lync servers have been removed from the guide.

MatchUri Set to IM and Presence Service Domain

This documentation update resolves CSCuh55035.
The definition for the MatchUri field was updated in the procedure titled *Configure Lync static route to point to IM and Presence Service*. The MatchUri value you enter must match the IM and Presence Service domain. This should also match the Line Server URI value that is specified for each user in the Lync Control Panel.

The MatchUri value must be written in double quotation marks, for example: -MatchUri "my-domain.com".

Use TLS for Static Routes

This documentation update resolves CSCui01368.

You must use TLS for static routes with Microsoft Lync servers. The TCP option for static routes between Microsoft Lync servers and IM and Presence Service was removed and some sections restructured.

Real-Time Monitoring Tool Guide

Alert Removal

This documentation update resolves CSCui25367.

The following alerts have been removed from Unified RTMT but are listed in the *Cisco Unified Real-Time Monitoring Tool Administration Guide*:

LowAttendantConsoleServerHeartbeatRate

LowCallManagerHeartbeatRate

LowTFTPServerHeartbeatRate

CallProcessingNodeCpuPegging Alerts for VMware Installations

This documentation update resolves CSCtu18692.

Cisco Unified Communications Manager VMware installations can experience high CPU usage spikes while performing tasks such as DRF backups and Bulk Administration Tool exports. The processes that are commonly responsible for CPU usage spikes are gzip and DRFLocal.

If your system is generating CallProcessingNodeCpuPegging alarms, add an additional vCPU for the support of 7500 Cisco Unified Communications Manager users following the Open Virtualization Archives (OVA) template specifications for your system.

The CallProcessingNodeCpuPegging alert is generated during CPU usage spikes. Other alarms that may also be issued during these CPU usage spikes include CoreDumpFound, CriticalServiceDown, SDLLinkOutOfService, and NumberOfRegisteredPhonesDropped alarms.

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 12: 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%)

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%.

Missing Content from Mailbox Sync Counters

This documentation update resolves CSCul36067.

The following counter information is missing:

The following table contains information about Mailbox Sync counters.

Counters	Counter Description
Active thread count	Cisco Unity Connection maintains threads for synchronization of voicemail from Cisco Unity Connection to Exchange server and vice-versa. At any moment, this counter specifies the number of threads that are actively in use for voicemail synchronization.
Background queue size	Mailbox sync has three types of priority queues: Background, Normal, and Time-Sensitive. Background queue is the lowest priority queue. This queue has items that are scheduled because of background re-synchronization of each mailbox hourly.
Normal queue size	Normal queue has moderate priority. This queue has items that are scheduled because of messaging operation (such as message CREATE, READ, UNREAD, DELETE) performed by user or any configuration update by administrator on Unified Messaging page on Cisco Unity Connection Administration.
Time sensitive queue size	Time sensitive queue has highest priority. This queue has such items that are scheduled because of keep-alive message sent by Cisco Unity Connection to Exchange server to keep subscription alive. This is applicable for 2003 Exchange server only.
Total connection errors	It specifies the number of times the CuMbxSync process fails to retrieve or update some data from database.
Total Mailbox Adds	It specifies the number of times a user mailbox has been setup for subscription. Any communication error between Unity Connection and Exchange, results in user mailbox remove and re-add.
Total Mailbox Removes	It specifies the number of times a user mailbox has been setup for un-subscription. Any communication error between Unity Connection and Exchange, results in user mailbox remove and re-add.

Counters	Counter Description
Total Resyncs	It specifies the total number of times user mailbox is resynchronized with Exchange server. Cisco Unity Connection does background resynchronization for all the user mailboxes hourly.
Total Retries	Whenever there is a communication failure between Cisco Unity connection and Exchange server, Unity Connection does mailbox synchronization retry for particular user mailbox. This counter specifies the count of such occurrences.
Total Work Items	It specifies number of times any messaging operation, such as CREATE, READ, UNREAD, and DELETE, has been performed on any user mailbox.

RTMT Cannot Collect OPC Logs Under Default Settings

This documentation update resolves CSCtw78204.

If you are using Cisco Unified Real-Time Monitoring Tool (RTMT) to monitor Cisco Unified Contact Center Enterprise, RTMT cannot collect OPC logs under the default settings. This issue arises because the default timeout for RTMT log collection is 60 seconds, but the OPC log collection process takes longer.

To resolve the issue, open the `<RTMT_INSTALLATION_FOLDER_PATH>/conf/rtmt.xml` file from the RTMT installation folder and change the value for ReadTimeout to 360. After you make the change, RTMT will be able to collect OPC logs.

Security Guide

BAT User Template Only Accepts Hexadecimal Characters for Digest Credentials

This documentation update resolves CSCul78860.

The table in “End user digest credential settings” sub section of “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.

Bulk Certificate Import May Cause Phones To Restart

This documentation update resolves CSCun32117.

The following note is omitted from the Bulk certificate export section in the *Cisco Unified Communications Manager Security Guide* and the Configure EMCC section in the *Cisco Unified Communications Manager Features and Services Guide*.

Note When you use the Bulk Certificate Management tool to import certificates, it will cause an automatic restart of the phones on the cluster on which you imported the certificate.

CTL File Size Limit Correction

This documentation update resolves CSCud57169.

The *Cisco Unified Communications Manager Security Guide* states the following: "The Cisco CTL Client limits the file size of a CTL file to 32 kilobytes because the phones cannot accept a larger CTL file." The file size limit should be 64 kilobytes.

Encryption Protocols Specifications Missing for Phone Models

This documentation update resolve CSCuo01831.

You can encrypt the phone configuration file for the following Cisco Unified IP Phones:

Phone Model and Protocol	Encryption Method
Cisco Unified IP Phone 7905G or 7912G (SIP only)	Manual key distribution—Encryption algorithm: RC4Key size: 256 bits File signing support: No
Cisco Unified IP Phone 7940G or 7960G (SIP only)	Manual key distribution—Encryption algorithm: Advanced Encryption Standard (AES) 128Key size: 128 bits File signing support: These phones that are running SIP receive signed, encrypted configuration files but ignore the signing information.

Phone Model and Protocol	Encryption Method
Cisco Unified IP Phone 6901, 6911, 6921, 6941, 6945, and 6961 Cisco Unified IP Phone 7970G, 7971G, or 7975G; Cisco Unified IP Phone 7961G, 7962G, or 7965G;Cisco Unified IP Phone 7941G, 7942G, or 7945G;Cisco Unified IP Phone 7911G; Cisco Unified IP Phone 7906G Cisco Unified IP Phone 7971G-GE, 7961G-GE, 7941G-GE Cisco Unified IP Phone 7931G, 7921G, 7925G, 7926G (SCCP only) Cisco Unified IP Phone 8941 and 8945 Cisco Unified IP Phone 8961, 9951, and 9971	Symmetric key encryption with phone public key (PKI encryption)—Encryption algorithm: AES 128Key size: 128 bits File signing support: Yes

Refresh Upgrade Update

The following content is missing from the “Refresh upgrade from Cisco Unified Communications Manager Release 7.x to Release 8.6 or later” section:

Once the publisher is up after the upgrade, do not reboot until the CAR migration completes. You are not allowed to switch to old version or perform a DRS backup in this phase. You can monitor the CAR migration status by navigating to **Cisco Unified Serviceability** > **Tools** > **CDR Analysis and Reporting**.

Secure Call Monitoring and Recording Update

This documentation update resolves CSCuj71412.

The note in “About secure call monitoring and recording setup”section is updated to remove the word “Secure” as the system does not support recording on authenticated phones.

Note The system does not support recording on authenticated phones.

SSL and TLS Support

This documentation update resolves CSCuf49157.

Cisco Unified Communications Manager supports SSL and Transport Layer Security (TLS) for HTTPS connections. Cisco recommends using TLS for improved security if your web browser version supports TLS. Disable SSL on your web browser to use TLS for secure HTTPS communications.

Updated Note for Rollback Cluster to Pre-8.0

This documentation update resolves CSCuf34403.

The note in step 1 of "Roll back cluster to a pre-8.0 release" section incorrectly states "pre-8.6". It is "pre-8.0".

Incorrect Configuration Example for ASA Router

This documentation update resolves CSCuv20903.

The "Configure ASA for VPN Client on IP Phone" procedure in the "VPN Client" chapter provides an example to configure an IOS router instead of an ASA router.

The following procedure contains the correct example.

Procedure

Step 1 Complete the local configuration.

a) Configure network interface.
Example:

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.89.79.135 255.255.255.0
ciscoasa(config-if)# duplex auto
ciscoasa(config-if)# speed auto
ciscoasa(config-if)# no shutdown
ciscoasa#show interface ip brief (shows interfaces summary)
```

b) Configure static routes and default routes.
ciscoasa(config)# **route** <interface_name> <ip_address> <netmask> <gateway_ip>

Example:

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.89.79.129
```

c) Configure the DNS.
Example:

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67
209.165.201.6
```

Step 2 Generate and register the necessary certificates for Cisco Unified Communications Manager and ASA. Import the following certificates from the Cisco Unified Communications Manager.

- CallManager - Authenticating the Cisco UCM during TLS handshake (Only required for mixed-mode clusters).
- Cisco_Manufacturing_CA - Authenticating IP phones with a Manufacturer Installed Certificate (MIC).

- CAPF - Authenticating IP phones with an LSC.

To import these Cisco Unified Communications Manager certificates, do the following:

a) From the Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
b) Locate the certificates Cisco_Manufacturing_CA and CAPF. Download the `.pem` file and save as a `.txt` file.
c) Create trustpoint on the ASA.
Example:

```
ciscoasa(config)# crypto ca trustpoint trustpoint_name
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate trustpoint_name
```

When prompted for base 64 encoded CA Certificate, copy-paste the text in the downloaded `.pem` file along with the BEGIN and END lines. Repeat the procedure for the other certificates.

d) Generate the following ASA self-signed certificates and register them with Cisco Unified Communications Manager, or replace with a certificate that you import from a CA.

- Generate a self-signed certificate.

  Example:

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>

ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# keypair <name>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- Generate a self-signed certificate with Host-id check enabled on the VPN profile in Cisco Unified Communications Manager.

  Example:

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>

ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# fqdn <full domain name>
ciscoasa(config-ca-trustpoint)# subject-name CN=<full domain
name>,CN=<IP>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- Register the generated certificate with Cisco Unified Communications Manager.

  Example:

```
ciscoasa(config)# crypto ca export <name> identity-certificate
```

Copy the text from the terminal and save it as a .pem file and upload it to the Cisco Unified Communications Manager.

Step 3 Configure the VPN feature. You can use the Sample ASA configuration summary below to guide you with the configuration.

Note To use the phone with both certificate and password authentication, create a user with the phone MAC address. Username matching is case sensitive. For example:

```
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB password
k1kLGQIoxyCO4ti9 encrypted
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB attributes
ciscoasa(config-username)# vpn-group-policy GroupPhoneWebvpn
ciscoasa(config-username)#service-type remote-access
```

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

Audit Log Configuration Settings

This documentation update resolves CSCub37263.

A caution was added at the end of the Audit Log Configuration Settings table.

Caution When enabled, database logging can generate large amounts of data in a short period, particularly if the debug audit level is set to **Database Updates** or **Database Reads**. This can result in a significant performance impact during heavy usage periods. In general, we recommend that you keep database logging disabled. If you do need to enable logging to track changes in the database, we recommend that you do so only for short periods of time, by using the **Database Updates** level. Similarly, administrative logging does impact on the overall performance of the web user interface, especially when polling database entries (for example, pulling up 250 devices from the database).

Audit Log Severity Levels

This documentation update resolves CSCua87708.

The following table displays descriptions for the audit log severity level codes.

Severity Code	Description
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

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.

CAR Database Update

This documentation update resolves CSCuv12448.

The CAR Database limit was entered as 6 GB. Updated the CAR Database setting to 3328 MB.

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 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.

User Options Logging

This documentation update resolves CSCuf16874.

A section for User Options events logging was added.

User logging (user login and user logout) events are logged for Cisco Unified Communications Manager User Options.

Platform Administrative Web Service

This documentation update resolves CSCup84833.

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

Platform Administrative Web Service

The Platform Administrative Web Service is a Simple Object Access Protocol (SOAP) API that can be activated on Cisco Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection systems to allow the PAWS-M server to upgrade the system.

Important Do not activate the Platform Administrative Web Service on the PAWS-M server.

SIP Transparency and Normalization Developers Guide

Cause Tag Required for convertHITоDiversion() API

This documentation update resolves CSCub77698.

If you are implementing the convertHITоDiversion() function with SIP Transparency and Normalization, a Diversion header will only be produced if the Histoy-Info header contains a "cause=" tag.

System Guide

Bandwidth Management Sections of Video Telephony in the 9.x System Guide

This documentation update resolves CSCue58676.

In the Differentiated Services Code Point (DSCP) packet marking, the following characteristic is added:

Video streams and associated audio streams in immersive video calls default to CS4 is added.

The following service parameter settings affect DSCP packet marking for media RTP streams are added:

- DSCP for Audio Portion of Video Calls
- DSCP for TelePresence Calls
- · DSCP for Audio Portion of TelePresence Calls

DSCP for ICCP Protocol Links is removed.

Call Preservation Support for SIP Trunks

This documentation update resolves CSCuc23992.

The Call Preservation feature in Cisco Unified Communications Manager supports SIP trunks. Active calls that cross a SIP trunk do not get interrupted when a Cisco Unified Communications Manager node fails, or when communication between a device and its cluster node fails

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.

LDAP Synchronized and Local End Users

This documentation update resolves CSCud14874.

This update applies to the End Users section in the *Cisco Unified Communications Manager System Guide*.

In the Cisco Unified Communications Manager, you can add end users in two ways:

- Manually create them in the database
- Automatically import them from the corporate LDAP directory

When LDAP synchronization is enabled, the local users are still active and after performing a synchronization, users that are imported from the LDAP directory are also active.

Phones that Support International Escape Character

This documentation update resolves CSCuj60918.

The up-to-date list of phones that support International Escape Character is as follows:

- Cisco Unified SIP Phones 3900 Series (3905, 3911)
- Cisco Unified IP Phones 6900 Series (6921, 6941, 6961, 6945)
- Cisco Unified IP Phones 7900 Series (7942, 7945, 7962, 7965, 7975, 7931)
- Cisco Unified IP Phones 8800 Series (8831)

- Cisco Unified IP Phones 8900 Series (8941, 8945, 8961)
- Cisco Unified IP Phones 9900 Series(9951, 9971)
- EX60, EX90, MX200, MX300

Presentation Sharing Supported with BFCP

This documentation update resolves CSCuh70981.

The *Cisco Unified Communications Manager System Guide* incorrectly states that Binary Floor Control Protocol (BFCP) is not supported when used between Cisco Unified Communications Manager and a Cisco TelePresence MCU conference bridge.

Cisco Unified Communications Manager supports presentation sharing with BFCP between Unified Communications Manager and a Cisco TelePresence MCU.

SCCP Device Handles One Call in a Pending State

This documentation update resolves CSCto78373.

You can use the Computer Telephony Integration application, known as the CTI application, to control Cisco Unified IP Phones.

For phones that are running SCCP, outbound dialing supports enbloc (the phone collects all digits before passing them to Cisco Unified Communications Manager for routing) or digit-by-digit collection. If dialing is done digit-by-digit, a CTI dialing call state notification gets sent to the phone when it goes off hook and the first digit is pressed for an outgoing call. For enbloc outbound dialing, the dialing call state notification gets delayed until the phone collects all the digits and sends them to Cisco Unified Communications Manager for routing.

When an outbound call is pending on an SCCP device and is not yet connected, Cisco Unified Communications Manager does not process call setup requests for that device until the first call is connected. If you are using a CTI application for outbound dialing, Cisco recommends that you configure an interval between outbound calls to ensure that pending calls are connected before new call requests are initiated.

SIP Redirect by Application Requires a SIP Route Pattern

This documentation update resolves CSCub17607.

If the Redirect by Application check box in the SIP Profile Configuration window is checked, Cisco Unified Communications Manager passes the Contact header of the redirection request through its routing engine and applies routing logic to forward the redirection request to the address in the Contact header. If the host portion of the Contact header is not a local Unified CM, a SIP route pattern may be required to map the host portion of the Contact header to an outgoing trunk or Unified CM will not be able to route the call.

For detailed information on how Unified CM routes SIP requests, see "Routing of SIP Requests in Unified CM" in the Dial Plan chapter of the *Cisco Unified Communications System SRND*.

Transcoding G.711 to All Codecs Supported

This documentation update resolves CSCtb31860.

The transcoder supports transcoding between G.711 and all codecs, including G.711, when functioning as a transcoder and when providing MTP/TRP functionality.

Trunk Types

This documentation update resolves CSCue75498.

Step 14 of the Set up SIP trunk procedure in the Cisco Unified Communications Manager System Guide states "When you enable Send send-receive SDP in mid-call INVITE for an early offer SIP trunk in tandem mode, Cisco Unified Communications Manager inserts MTP to provide sendrecv SDP when a SIP device sends offer SDP with a=inactive or sendonly or recvonly in audio media line." This statement incorrectly qualifies the situation as occurring in tandem mode only. This situation can occur for all clusters.

Video Resolution Support for SIP Phones

This documentation update resolves CSCuf57901.

Cisco Unified Communications Manager supports the imageattr line in the Session Description Protocol (SDP) portion of the SIP header for higher resolution video calls. Cisco SIP phones that support w360p (640 x 360), such as the 9951, 9971, and 8961, automatically select the best resolution for video calls depending on the following criteria:

- If the session level bandwidth is greater than 800 Kbps and the imageattr[640 x 480] line in the SDP exists, then VGA is used.
- If the session level bandwidth is greater than 800 Kbps and the imageattr[640 x 480] line in the SDP does not exist, then w360p is used.
- If the session level bandwidth is less than 800 Kbps but greater than 480 bits per second and the imageattr[640 x 480] line exists, then VGA 15 frames per second is used.

Note If you currently have a Cisco Unified IP Phone model 9951, 9971, or 8961 that supports w360p (640 x 360) video resolution and are upgrading to Cisco Unified Communications Manager Release 8.5(1) or later, you may notice changes in the resolution of video calls.

The following video call flow is between two 9951 phones (Phone A and Phone B) without imageattr line support (for example, using Cisco Unified Communications Manager Releases 8.0(1) and earlier):

1. Phone A sends a SIP message with an imageattr line in the SDP.
2. Cisco Unified Communications Manager deletes the imageattr line in the SDP and then sends the modified SIP message to Phone B.
3. Phone B attempts to send video with the w360p resolution because there is no imageattr line in the SDP portion of the SIP header.

The following video call flow is between two 9951 phones (Phone A and Phone B) with imageattr line support (for example, using Cisco Unified Communications Manager Releases 8.5(1) and later):

1. Phone A sends a SIP message with the imageattr line in the SDP.
2. Cisco Unified Communications Manager does not delete the imageattr line and sends the SIP message to Phone B unchanged.
3. Phone B attempts to send video with the VGA resolution.

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

Port Information for UDS

This documentation update resolves CSCuc77135.

The *TCP and UDP Port Usage for Cisco Unified Communications Manager* document does not mention port usage information for Cisco User Data Services. Endpoints can make a TCP connection to Cisco Unified Communications Manager port 8443 for Cisco User Data Services requests.

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

Adding a New Subscriber Causes Device Reset

This documentation update resolves CSCub12922.

After you install a new node in an existing cluster, all phones that are registered to the cluster are reset.

Downtime When Upgrading Publisher Server Until All Subscriber Servers Are Updated

This documentation update resolves CSCtd69640.

When upgrading the publisher node, there will be a temporary server outage until all subscriber nodes get upgraded to the new software version.

Preupgrade Step to Check Connectivity

This documentation update resolves CSCue26921.

The pre-upgrade step to check the connectivity between the IM and Presence Service server and Cisco Unified Communications Manager was added to the *Upgrade Guide for Cisco Unified Communications Manager*.

Problem During an IM and Presence Service upgrade, the IM and Presence Service server generates the following error message, even though the upgrade path and file are valid.

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

Solution The upgrade manager checks for connectivity between IM and Presence Service and Cisco Unified Communications Manager to validate the version during the upgrade. If this fails, the IM and Presence Service server generates the error message even though the upgrade path and file are valid. Use a tool, such as the Cisco Unified CM IM and Presence Administration System Troubleshooter, to check that there is connectivity between IM and Presence Service and Cisco Unified Communications Manager before proceeding with the upgrade.

Presence Data Loss After Upgrade From Cisco Business Edition 5000 to Cisco Unified Communications Manager

This documentation update resolves CSCts65285.

There is no upgrade path in VMware to upgrade from Cisco Business Edition 5000 to Cisco Unified Communications Manager. A fresh installation is needed. After you perform the fresh installation, IM and Presence Service resynchronizes data with the new Cisco Unified Communications Manager. The Syncagent uses the primary key (pkid) as a comparison field for the synchronization. When the Cisco Unified Communications Manager is reinstalled, all the pkids on Cisco Unified Communications Manager are changed. As such, any existing data on IM and Presence Service is cleaned up and the Syncagent deletes the old data.

Caution Be sure to back up your data before performing this procedure.

Presence User Experiences Issues Obtaining Availability

This documentation update resolves CSCto77824.

After an IM and Presence Service server upgrade, when all activated feature services and network services are started, a user experiences inconsistent presence availability. The user can log in to IM and Presence Service but will experience issues obtaining availability information, mainly from SIP-based clients.

This issue is caused when users are provisioned while IM and Presence Service is being upgraded. You must unassign and then reassign the user.

User Options Guide

The Fast Dial User Option is Not Supported

This documentation update resolves CSCuf57054.

The “Add Contact” procedure states that you can configure fast dial information while adding a contact. This statement is incorrect as Cisco Unified CM User Options supports speed dials, but not fast dials.

XML Developers Guide

MaxReturnedDevices in Serviceability XML

This documentation update resolves CSCup71020.

The *Cisco Unified Communications Manager XML Developers Guide, Release 9.0(1)* incorrectly specifies the maximum number of devices (MaxReturnedDevices) for which information can be returned in a search as 1000. The correct maximum number of devices is 200.

Serviceability XML API Doc in Error

This documentation update resolves CSCum01216.

The following is implemented in Cisco Unified Communications Manager in Release 10.0(1):

The SelectCmDevice API returns SIP trunk status and also returns the IP addresses and status of the peer devices.

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*.

Online Help for Cisco Unified Communications Manager

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.

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.