Release Notes for Cisco Unified Communications Manager and IM and Presence Service, Release 9.1(1)

First Published: December 20, 2012

Last Modified: October 05, 2013

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-28258-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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)

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface xi

Purpose xi

Organization xii

Audience xii

Conventions xiii

Obtain Support xiv

CHAPTER 1

Introduction 1

Hardware Server Requirements 1

Server software requirements 4

Supported browsers 4

CHAPTER 2

Upgrading to Unified CM 9.1(1) 5

Software Version Number 5

Pre-Upgrade Tasks 5

Overview of Software Upgrade Process 7

Upgrading on a Virtual Server 8

Configuration Changes During Upgrade 9

Supported Upgrades 9

Upgrade File 9

Upgrade Media 9

Software Upgrade Procedures 10

Install the COP File 10

Upgrade to Restricted or Unrestricted Unified Communications Manager 10

Upgrade From a Local Source 10

Upgrade From a Remote Source 12

Supported SFTP Servers 12

Bridge Upgrade 14
Post-Upgrade Tasks 14
Latest Software and Firmware Upgrades 15
Firmware 15
Software 15
Related Documentation 15
Limitations and Restrictions 16

CHAPTER 3 Upgrading to IM and Presence 9.1(1) 17
New system installation information 17
System Upgrade 17
Supported Upgrade Paths to IM and Presence Service Release 9.1(1) 17
Upgrade from Cisco.com 18
Upgrade order 19
Software licensing requirements for VMware 19
Recommendations for Release 8.0(x), 8.5(x), or 8.6(x) to 9.1(1) Upgrades 19

CHAPTER 4 Important Notes 21
BFCP is Supported with TelePresence MCU 22
Native Call Queuing Periodic Announcement Behavior 22
Disable Empty TLS Fragments 22
Adding a New Subscriber Causes Device Reset 22
EMCC Logout Limitation 23
Call Queuing Interaction with Hunt Groups and Hunt Pilots 23
Bandwidth Management Sections of Video Telephony in the 9.x System Guide 23
Cannot Install Signed Microsoft CA Server-Client Authentication Certificate on Microsoft OCS 2008 23
Presence Data Loss After Upgrade From Cisco Business Edition 5000 to Cisco Unified Communications Manager 24
Presence User Experiences Issues Obtaining Availability 24
Access Control Group Permissions Interactions 24
CallProcessingNodeCpuPegging Alerts for VMware Installations 25
Centralized Proxy TFTP File Signature Verification Failure 25
Empty Far-End When Recording Call Park for Some Phones 25
Limitation for Mobility Voice Mail Avoidance 25

Upgrade to 9.1(1) Fails with Insufficient Disk Space 26
Reduce Disk Space Utilization 26
Cisco Prime Unified Provisioning Manager Business Edition Compatibility 27
Phone Support for URI Dialing Display Preference Service Parameter 28
Call Queuing Not Supported with Mobile Device Types 28
CSCug39491 Configure Cygwin with DRS 28
CSCui95074 The Release Note for RTMT Does Not Mention Win7 as Supported Platform 28
Bridge Upgrade Fails with Insufficient Disk Space 28
Corrections for the Immediate Divert Feature 29
Bulk Certificate Import Can Cause Phones to Restart 30
CSCup71020 MaxReturnedDevices in Serviceability XML 30
Browser Support for Cisco Unified CM User Options 30
Show perf query counter Command Output 30

CHAPTER 5 New and Changed Information 33
Feature Enhancements in Release 9.1(1) 33
Paging 35
Cisco Jabber Support for Single Sign-On 36
Enhanced IM and Presence Deployment Support 36
Partitioned Intradomain Federation with Microsoft Lync 36
Licensing 36

CHAPTER 6 Caveats 39
Bug Search Tool 39
Resolved Caveats 40
Open Caveats 40
Open Caveats for Unified Communications Manager Release 9.1(1) 41
Open Caveats for IM and Presence Service Release 9.1(1) 45
Open Caveats for Enterprise License Manager 9.1(1) 47

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 50
Call Stats Field Removed 51
Common Phone Profile Settings Secure Shell Information 51
Connected Lined ID Presentation Value 51
CTI Remote Device Name Cannot Contain Spaces 51
Directory Number Line Behavior in Cisco Unified Communications Manager 51
Hostnames in IPv4 and IPv6 Environments 51
An ILS Restart is Required for Changes to Directory URI Catalogs 52
Incorrect Information about Deleting Route Patterns 52
Incorrect Note about User Locales 52
Line Group Deletion Correction 53
Maximum Hunt Timer Restriction 53
Link Loss Type Field is Relabeled 53
Option For Voicemail Usage Description 53
Service Name Cannot Be Localized 54
Use Personal Preference Field is Relabeled 54
Directory Number Field Description Updated 54
Bulk Administration Guide 54
Missing Note in Insert Phone Topic 54
Model Is Not a Valid Device Field When Generating Phone Reports 55
Call Detail Records Administration Guide 55
Call Recording Samples in CDR Examples Chapter 55
Change Order of HuntPilotDN 57
FinalCalledPartyNumber Field Description Is Incorrect 57
Missing CDR Field Descriptions 57
Missing CDR Field Descriptions for IMS Application Server 57
Changing IP Address and Hostname 59
Change the Hostname Using the Unified Communications Operation System Administration GUI 59
Database Replication After Hostname Change 60
Do Not Change the Hostname and IP Address Together 60
Error in the Procedure for Changing the Hostname 60
IP Address, Domain and Hostname for IM and Presence Service 60
set network ip eth0 Requires Gateway Parameter 60
CLI Reference Guide 61

Enable or Disable FIPS for IM and Presence Service 61
ILS Troubleshooting Tips Corrections 61
run cuc sysagent task Example is Incorrect 61
set network domain Conflicting Information 61
Show perf query counter Command Output 62
Deployment Guide for IM and Presence Service 62
Enhanced IM and Presence Deployment Support 62
Exceeding Maximum Contact List Settings During Contact List Import Is Supported 63
Locale Installation Information Update 63
Disaster Recovery System Guide 63
Supported SFTP Servers 63
System Backup File Encryption 64
Updated Caution to Include DNS and Domain Name Prior To Restore 64
Features and Services Guide 65
Call Mobility Missing Information 65
Call Park Display Timer Restriction 65
Call Pickup Group Visual Notification Does Not Support Localization 65
Call Pickup Phones Supported 65
Call Queuing Interaction with Hunt Groups and Hunt Pilots 65
Call Queuing Missing Information 65
Call Queuing Not Supported with Mobile Device Types 66
Call Queuing Shared Line Scenario Description 66
Calling Party Normalization Restriction 66
Centralized Proxy TFTP File Signature Verification Failure 66
Configuring OpenAM Section 67
Corrections for the Immediate Divert Feature 68
EMCC Incorrect Limitation 68
EMCC Logout Limitation 69
EMCC Remote Cluster Menu 69
EMCC Video Calling Override Common Settings 69
Empty Far-End When Recording Call Park for Some Phones 69
Enterprise Feature Access and User Control 69
Extension Mobility Equivalency Changes 70
Extension Mobility Now Supports Device Owners 71
Hunt Pilots Limit for a Call Queue 71

Jabber Devices Count as Registered Devices 71
Licensing Usage Report Correction 71
Locale Usage for Queue Announcements Clarification 72
MGCP FXS Ports Do Not Require a License 72
Music On Hold and Native Call Queuing Behavior 73
Native Call Queuing Periodic Announcement Behavior 73
Play Continuously and Music On Hold 73
Remote Destination and Auto Answer 73
SIP Phones Support CMC and FAC Tones 73
IM and Presence Administration Online Help 74
Microsoft Lync and FQDN Updates 74
Extension Mobility Now Supports Device Owners 74
XMPP Certificate Settings Section Missing 74
Installing Cisco Unified Communications Manager 75
Add a New Node to an Existing Cluster 75
Change the IM and Presence Node Name 75
External NTP Server Requirements 75
Installation Fails with Unrecoverable Internal Error 75
Interdomain Federation for IM and Presence Service 76
Cannot Install Signed Microsoft CA Server-Client Authentication Certificate on Microsoft OCS 2008 76
FIPS Not a Requirement for Federated Connections with LYNC 2010 Servers 77
Microsoft Lync Support 77
Use TLS for Static Routes 77
Managed Services Guide 77
Unified Communications Manager Alarms 77
Migration and Upgrade Guide 78
Server Support 78
OS Administration Guide 78
Client Profile Agent Update 78
Documentation Update for Certificate Monitor Configuration 78
ICSA Service Needs Restart After Ipsec Cert Is Regenerated 78
Partitioned Intradomain Federation for IM and Presence Service 79
Disable Empty TLS Fragments 79
FIPS Not a Requirement for Federated Connections with LYNC 2010 Servers 79

MatchUri Set to IM and Presence Service Domain 79
Use TLS for Static Routes 79
Real-Time Monitoring Tool Guide 79
Alert Removal 79
Audit Log Configuration Settings 80
CallProcessingNodeCpuPegging Alerts for VMware Installations 80
Incorrect Default Value for LogPartitionLowWaterMarkExceeded Alert 80
Missing Content from Mailbox Sync Counters 81
An RTMT Update Is Required When You Upgrade Unified CM 82
Upgrade RTMT 82
User Options Logging 83
Security Guide 83
BAT User Template Only Accepts Hexadecimal Characters for Digest Credentials 83
Bulk Certificate Import Can Cause Phones to Restart 83
CTL File Size Limit Correction 84
Encryption Protocols Specifications Missing for Phone Models 84
Refresh Upgrade Update 85
Secure Call Monitoring and Recording Update 85
SSL and TLS Support 85
Updated Note for Rollback Cluster to Pre-8.0 86
Serviceability Guide 86
AXL Web Service Requirement for ICSA HA 86
Cisco CAR DB Service 86
Cisco SOAP-CallRecord Service 86
SOAP-Diagnostic Portal Database Service 87
Platform Administrative Web Service 87
System Guide 87
Configure LDAP Directory 87
Connected Lined ID Presentation Value 88
LDAP Synchronized and Local End Users 88
Phones that Support International Escape Character 88
Phones That Support Private Line Automatic Ringdown 88
Presentation Sharing Supported with BFCP 89
TFTP Cisco SIP Phones 89
Updates to Supported Cisco Unified IP Phones 89

Video Resolution Support for SIP Phones 96
TCP and UDP Port Usage Guide 97
Destination Listener port value for IM and Presence 97
Ports Between Unified CM and LDAP 97
Missing Information about TCP Port 22 97
Missing Information about TCP Port 5555 98
User Options Guide 98
The Fast Dial User Option is Not Supported 98
Upgrade Guide 98
Adding a New Subscriber Causes Device Reset 98
Preupgrade Step to Check Connectivity 98
Presence Data Loss After Upgrade From Cisco Business Edition 5000 to Cisco Unified Communications Manager 99
Presence User Experiences Issues Obtaining Availability 99
XML Developers Guide 100
CSCup71020 MaxReturnedDevices in Serviceability XML 100
Serviceability XML API Doc in Error 100

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 xi
- Organization, page xii
- Audience, page xii
- Conventions, page xiii
- Obtain Support, page xiv

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.

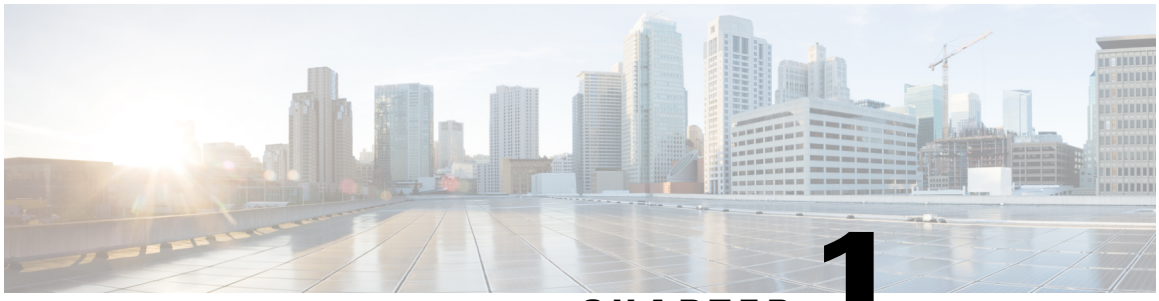
Warnings use the following conventions:

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 15 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 Service.

Server Support for Cisco Unified Communications Manager

Make sure that you install and configure Unified Communications Manager and IM and Presence Service 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 Communications Manager or IM and Presence Service, see the related compatibility matrix.

- *Hardware and Software Compatibility Information for IM and Presence Service on Cisco Unified Communications Manager*: 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.

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* here: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/port/9_0_1/CUCM_BK_CCBD7A20_00_cucm-tcp-udp-port-usage.html.

The IM and Presence Service 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 Service supports bridge 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 72 GB of storage space; otherwise it is fully supported)
- MCS-7845-I1-IPC1

The bridge 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 Service installation on the supported hardware. If you attempt an upgrade on discontinued hardware, a warning appears on the interface and on the CLI, informing you that Unified Communications Manager or IM and Presence Service supports only the functionality to create a DRS backup on this server.

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

Uninterruptible Power Source

Cisco recommends that you connect each Unified Communications Manager or IM and Presence Service 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 any cached data is lost during a power outage on these servers with drive write cache enabled (and no internal RAID cache battery backup). To prevent such file system corruption, you must connect these servers to a UPS.

When Unified Communications Manager and IM and Presence Service run on one of the servers listed in the table below, basic integration to UPS models APC Smart-UPS 1500VA USB and APC 750VA XL USB is supported.

This integration occurs through a single point-to-point USB connection. Serial and SNMP connectivity to the 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 are supported with the APC Smart-UPS 1500VA USB and APC 750VA XL USB. The feature activates automatically during bootup if a connected UPS is detected.

Alternatively, you can run 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 integration feature is activated, graceful shutdown begins as soon as the low-battery threshold is reached. Resumption or fluctuation of power will not interrupt or cancel the shutdown, and administrators cannot stop the shutdown after the integration feature is activated.

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

Table 2: Supported Servers for UPS Integration

HP servers	IBM servers
MCS-7816-H3	MCS-7816-I3
MCS-7825-H3	MCS-7816-I4
MCS-7825-H4	MCS-7816-I5
MCS-7828-H3	MCS-7825-I3
MCS-7835-H2	MCS-7825-I4
MCS-7845-H2	MCS-7825-I5

HP servers	IBM servers
	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.

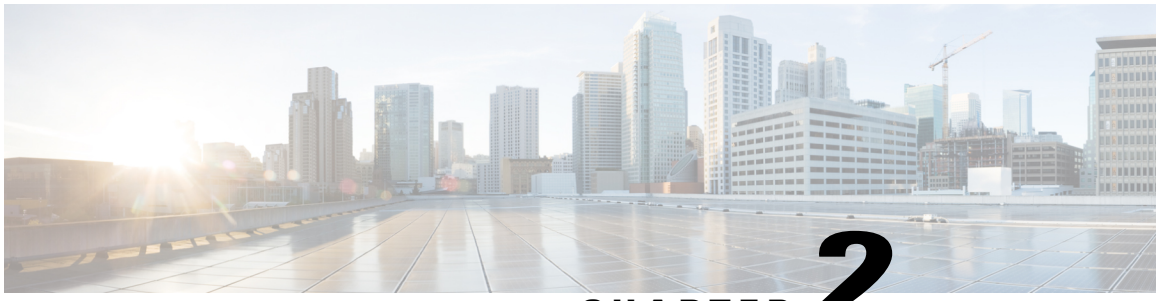
Supported browsers

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 9.1(1)

- Software Version Number, page 5
- Pre-Upgrade Tasks, page 5
- Overview of Software Upgrade Process, page 7
- Upgrading on a Virtual Server, page 8
- Configuration Changes During Upgrade, page 9
- Supported Upgrades, page 9
- Upgrade File, page 9
- Upgrade Media, page 9
- Software Upgrade Procedures, page 10
- Post-Upgrade Tasks, page 14
- Latest Software and Firmware Upgrades, page 15
- Related Documentation, page 15
- Limitations and Restrictions, page 16

Software Version Number

These release notes are based on the following software version:

- Unified Communications Manager: 9.1.1.10000-11

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.

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 9.1 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 9.1** > **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 10.

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 10.

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 10.
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 associated with supported applications:

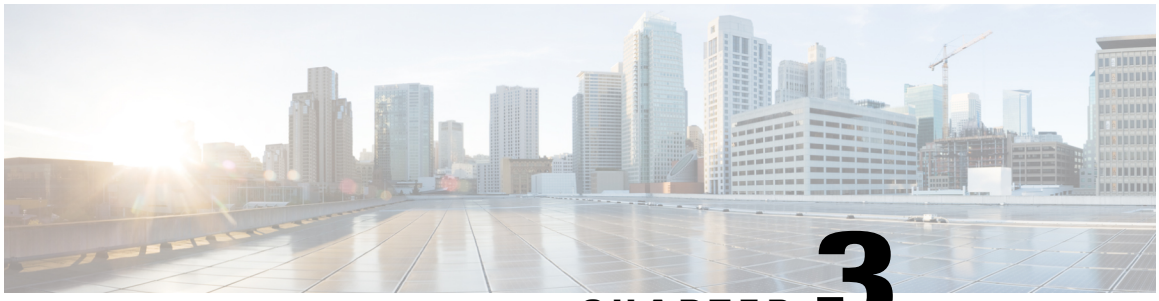
- Cisco Unified Communications Manager - http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
- Cisco Unified Contact Center Express - http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/tsd-products-support-series-home.html
- 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 9.1(1)

- New system installation information, page 17
- System Upgrade, page 17
- Upgrade order, page 19
- Software licensing requirements for VMware, page 19
- Recommendations for Release 8.0(x), 8.5(x), or 8.6(x) to 9.1(1) Upgrades, page 19

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 Service Release 9.1(1)

IM and Presence Service supports the following software upgrade paths to Release 9.1(1):

Supported Upgrade Paths from IM and Presence Service...	Installation Instructions
Release 8.0(1) through 8.6(x) and Release 9.0(1) to 9.1(1)	Upgrades from Release 8.0(1) through 8.6(1) to Release 9.1(1) require a Refresh Upgrade using the ciscocm.cup.refresh_upgrade_v1.01.cop.sgn file. Upgrades from Release 8.6(2) and 8.6(3) to Release 9.1(1) require a Refresh Upgrade only. Upgrades from Release 8.6(4), 8.6(5), and Release 9.0(1) to Release 9.1(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 9.1(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 9.1** > **Unified Presence Server (CUP) Updates-9.1(1)**. **3** Download the complete ISO file: UCSInstall_CUP_9.1.1.10000-8.sgn.iso

Note Direct upgrades from Cisco Unified Presence Release 6.0(x) to Release 9.1(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 9.1(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 9.1(1), Cisco strongly advises that you follow the recommended upgrade procedure in the *Upgrade Guide for Cisco Unified Communications Manager, Release 9.1(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**

  Before you perform an upgrade, this service may be disabled on the cluster (which only runs on the Publisher node). This action will ensure that user-initiated changes from the corresponding Unified Communications Manager system during the upgrade do not compromise the upgrade process. The changes are reconciled when the IM and Presence Service Sync Agent is restarted in either the current or newer version.

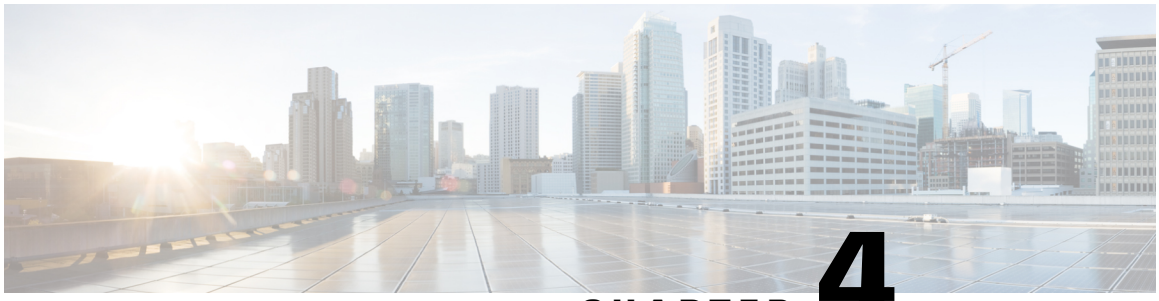
- **Publisher node**

  Switch versions and restart the publisher node before you begin 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 and restarted, and replication is successfully established on that cluster.

- **Contact List Size**

  The default maximum value is 200; however, you can use higher value or specify the value as 0 to set it to an 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 an IM and Presence Service node supports is reduced.



CHAPTER 4

Important Notes

- BFCP is Supported with TelePresence MCU, page 22
- Native Call Queuing Periodic Announcement Behavior, page 22
- Disable Empty TLS Fragments, page 22
- Adding a New Subscriber Causes Device Reset, page 22
- EMCC Logout Limitation, page 23
- Call Queuing Interaction with Hunt Groups and Hunt Pilots, page 23
- Bandwidth Management Sections of Video Telephony in the 9.x System Guide, page 23
- Cannot Install Signed Microsoft CA Server-Client Authentication Certificate on Microsoft OCS 2008, page 23
- Presence Data Loss After Upgrade From Cisco Business Edition 5000 to Cisco Unified Communications Manager, page 24
- Presence User Experiences Issues Obtaining Availability, page 24
- Access Control Group Permissions Interactions, page 24
- CallProcessingNodeCpuPegging Alerts for VMware Installations, page 25
- Centralized Proxy TFTP File Signature Verification Failure, page 25
- Empty Far-End When Recording Call Park for Some Phones, page 25
- Limitation for Mobility Voice Mail Avoidance, page 25
- Upgrade to 9.1(1) Fails with Insufficient Disk Space, page 26
- Cisco Prime Unified Provisioning Manager Business Edition Compatibility, page 27
- Phone Support for URI Dialing Display Preference Service Parameter, page 28
- Call Queuing Not Supported with Mobile Device Types, page 28
- CSCug39491 Configure Cygwin with DRS, page 28
- CSCui95074 The Release Note for RTMT Does Not Mention Win7 as Supported Platform, page 28
- Bridge Upgrade Fails with Insufficient Disk Space, page 28

- Corrections for the Immediate Divert Feature, page 29
- Bulk Certificate Import Can Cause Phones to Restart, page 30
- CSCup71020 MaxReturnedDevices in Serviceability XML , page 30
- Browser Support for Cisco Unified CM User Options, page 30
- Show perf query counter Command Output, page 30

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.

Native Call Queuing Periodic Announcement Behavior

This documentation update resolves CSCui20806.

The following information is omitted from the “Call Queuing” and “Music On Hold” chapters in the *Features and Services Guide*:

Initial announcements are always simulcast to each new caller. Periodic announcements are multicast to queued callers at the specified time interval. Callers who join the queue after the periodic announcement begins to play may only hear a portion of the announcement.

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.

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.

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.

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.

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.

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.

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.

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.

CallProcessingNodeCpuPeggingAlertsforVMwareInstallations

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.

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*.

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.

Limitation for Mobility Voice Mail Avoidance

This information applies to CSCud25228.

A possible limitation involves both Voice Mail Avoidance (VMA) and Call Forward No Answer (CFNA) interaction. The scenario is as follows:

CFNA Timer = 12 seconds

Delay Before Ring Timer = 4 seconds

Call Screening Timer = 4 seconds

User Control Confirmed Answer Indication Timer = 10 seconds

1. 00:00 Phone A calls a 3G-registered dual-mode device configured with user control voicemail avoidance, dual-mode B (DM B). This dual-mode has a shared line, Phone C.
2. 00:00 Phone A hears a ringback tone. The CFNA and Delay Before Ring timers start. Phone C rings.
3. 00:04 The Delay Before Ring timer pops. The mobility layer attempts to establish the 3G data channel before extending the call over the PSTN network. The SIP Progress timer (Call Screening timer) starts.
4. 00:08 The Call Screening timer pops. Due to 3G network errors or delays, the mobility layer never received a SIP Progress from the dual-mode mobile client. To make up for this, the CFNA timer is restarted. The call to the mobile identity of DM B is extended over the PSTN network.
5. 00:18 User answers the call on the mobile identity of DM B. The CFNA timer is restarted again. The user does not hear the prompt to "press any digit to be connected."
6. 00:28 The User Control Confirmed Answer Indication Timer fires. Mobility tears down the call and sends a CcRejInd. However, LineCdpc holds onto this CcRejInd because it has not heard from all other shared lines, including Phone C.
7. 00:30 The CFNA timer fires and Phone A is redirected to the voicemail/CFNA destination of DM B/Phone C.

Note Though unlikely, this scenario is possible. Cisco determined that it is preferable for users to have a lengthened CFNA timer than to have users pick up the call on their mobile identity with, for example, 2 seconds left on the CFNA timer. If the CFNA timer is not restarted and the user does not press a digit within 2 seconds, the call will suddenly be redirected to the CFNA destination, leaving the called user confused.

Upgrade to 9.1(1) Fails with Insufficient Disk Space

This information applies to CSCuc63312.

When upgrading Cisco Unified Communications Manager to Version 9.1(1), the upgrade may fail due to insufficient disk space. You will see the following error message:

There is not enough disk space in the common partition to perform the upgrade. For steps to resolve this condition please refer to the Cisco Unified Communications Manager 9.1(1) Release Notes or view defect CSCuc63312 in Bug Toolkit on cisco.com.

Reduce Disk Space Utilization

Follow this procedure to reduce disk space utilization during an upgrade.

Procedure

Step 1 Reduce the amount of traces on the system by lowering the low and high watermarks in the Cisco Log Partition Monitoring Tool. The low watermark adjusts by changing the properties of the LogPartitionLowWaterMarkExceeded alert. The high watermark adjusts by changing the properties of the LogPartitionHighWaterMarkExceeded alert.
For more information about the Cisco Log Partition Monitoring Tool, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Note After the upgrade, you must restore the high and low watermarks to their original values in order to avoid premature purging of traces. The default value for the high watermark is 85. The default value for the low watermark is 80.

Step 2 If you still get the error message, install the COP file named `ciscocm.free_common_space_v1.0.cop.sgn` that you can find on Cisco.com at **Cisco Unified Communications Manager Version 9.1** > **Unified Communications Manager/ CallManager/ Cisco Unity Connection Utilities** > **COP-Files**.
This COP file frees disk space to allow the upgrade to proceed.

Note You must perform an upgrade after applying the COP file.

Caution You will not be able to switch to the previous version after the COP file is installed. For example, if you are upgrading from Cisco Unified Communications Manager 9.0(1) to Cisco Unified Communications Manager 9.1(1) and the previous version is Cisco Unified Communications Manager 8.6, the COP file clears the space by removing the 8.6 version data that resides in the common partition. So after you apply the COP file, you will not be able to switch to the 8.6 version.

Note If you are unable to perform the upgrade and continue to receive the error message after applying this COP file, the amount of data present on the running version does not leave adequate space for expanding and executing the upgrade. In this case, you can recover more space by removing unused device firmware from the TFTP path. In some cases, having sufficient space for an upgrade will require that you take a backup, reinstall to a larger capacity disk or larger sized Open Virtual Appliance (OVA), and restore. Contact Cisco Technical Assistance Center (TAC) if you require further assistance.

Cisco Prime Unified Provisioning Manager Business Edition Compatibility

This information applies to CSCue09155.

Cisco Unified Communications Manager 9.1(1) is not compatible with Cisco Prime Unified Provisioning Manager Business Edition 9.0(1).

Phone Support for URI Dialing Display Preference Service Parameter

Most Cisco Unified IP Phones do not support the URI Dialing Display Preference service parameter. Regardless of how you configure the service parameter, the phone displays a directory URI, if one is available. To ensure full support of this service parameter, make sure that you install the latest phone builds. This service parameter is fully functional system-wide only after the phone firmware implements the changes.

Note The default value of URI Dialing Display Preference has been changed from "URI" to "DN."

Call Queuing Not Supported with Mobile Device Types

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

CSCug39491 Configure Cygwin with DRS

CSCui95074 The Release Note for RTMT Does Not Mention Win7 as Supported Platform

You can install Cisco Unified Real-Time Monitoring Tool (Unified RTMT) on a computer running Windows 7.

Note To create a Unified RTMT certificate store on a Windows 7 platform, you must have a username with full administrative privileges.

Bridge Upgrade Fails with Insufficient Disk Space

This information applies to CSCuj24138.

Bridge upgrades may fail due to insufficient disk space on servers that have 72GB hard drives, such as the MCS-7835-H2 or the MCS-7835-I2. When this failure occurs, the `install.log` file displays a message indicating that there is no more space left on the partition.

This failure may occur when you are upgrading a large cluster, when the database is large, or when the server contains a large amount of TFTP data. If a failure occurs when you upgrade from Cisco Unified Communications Manager Release 7.x to Release 9.1(1), perform one or more of the following actions to create more disk space on the partition:

- Move log files to other machines.
- Install the `ciscocm.free_common_space_<latest_version>.cop.sgn` file; this COP file removes the inactive side in the common partition to increase available disk space.

Note If you install the COP file, you will not be able to switch back to the inactive version.

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 3: 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 Model	Divert Softkey	iDivert Softkey	What to configure in softkey template
Cisco Unified IP Phone 9900 Series	X		iDivert

Bulk Certificate Import Can 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 causes an automatic restart of the phones on the cluster on which you imported the certificates.

CSCup71020 MaxReturnedDevices in Serviceability XML

The *Cisco Unified Communications Manager XML Developers Guide, Release 9.1(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.

Browser Support for Cisco Unified CM User Options

The following table displays the list of supported browsers for Cisco Unified CM User Options Release 9.1(1).

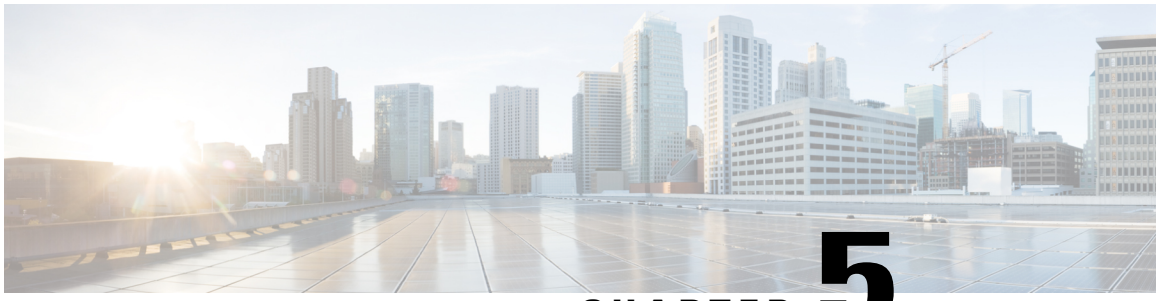
Platform	Windows XP	Windows 7	Windows 8
Supported Browser	Internet Explorer 8 Firefox 8, 9 Chrome 25	Internet Explorer 9 Firefox 8, 9 Chrome 25	Internet Explorer 8, 9 Firefox 8, 9 Chrome 25

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.



CHAPTER 5

New and Changed Information

- Feature Enhancements in Release 9.1(1), page 33
- Paging, page 35
- Cisco Jabber Support for Single Sign-On, page 36
- Enhanced IM and Presence Deployment Support, page 36
- Partitioned Intradomain Federation with Microsoft Lync, page 36
- Licensing , page 36

Feature Enhancements in Release 9.1(1)

The following table lists the feature enhancements in Unified Communications Manager Release 9.1(1).

Table 4: Feature Enhancements in Release 9.1(1)

Enhancement	Description
CBarge Unique Call ID	On 89XX and 99XX devices when using shared lines, the Unique Call ID tells users which calls to pick up. The Call ID will remain static for the duration of the conference. For details, see CSCub35904 in Bug Toolkit.
Increase Phone Service Field Characters	Increase character limit of the IP Phone Service Name field from 32 to 128 characters for Android applications to allow for longer application names. For details, see CSCty64623 in Bug Toolkit.
Original Call Classification for SIP	Making service parameter "Use Original Call Classification for Transferred Calls" effective when a SIP phone is transferring a call, as it is for SCCP phones. For details, see CSCty38858 in Bug Toolkit.

Support for VG350 gateway	VG350 is a new high density analog gateway which will support up to 160 analog lines in one box. This gateway will be configurable on Unified Communications Manager and will also have BAT support.
Scaling SAF learned routes	Increasing the Scale of Service Advertisement Framework (SAF) learned patterns from 20,000 to 100,000.
VG224 Security configuration	Having a configurable option on Unified Communications Manager for VG224 so that it can be marked "trusted" when configured using secure SCCP. For details, see CSCti08882 in Bug Toolkit.
Calling Party Normalization	Consistent Calling party information for globalized dial plans in case of features like call transfer. For details, see CSCtd09842 in Bug Toolkit.
Support Analog modules to ISR-G2	Configuration support in Unified Communications Manager to support 48 and 72 port analog cards analog ISR-G2 modules.
Enterprise License Management electronic fulfillment	Electronic fulfillment of Product Authorization Keys (PAKs) within Enterprise License Management. Customers can enter the PAKs in the Enterprise License Management service and the service will automatically download licenses. For details, see the *Enterprise License Manager User Guide*.
CCMCIP Throttling	Introduce a throttling mechanism to protect the Unified Communications Manager system during an overload of the Cisco CallManager Cisco IP Phone (CCMCIP) service component. For details, see CSCty20488 in Bug Toolkit.
Audio Only Lock Icon (ignore video)	A configurable option is introduced in Unified Communications Manager that will allow to customers to display lock icon (security icon) when only audio is secure and CUVA video is not secure. For details, see CSCua91582 in Bug Toolkit.
Commercial Licensing Changes	Implementation of the new licensing commercial model. For more details, refer to the "Licensing" section below, or see the *Enterprise License Manager User Guide*.

Automatically Logout Hunt Member on No Answer	Automatic logout of hunt members was introduced for queuing-enabled hunt pilots in Unified Communications Manager 9.0(1). If an agent does not answer a queuing-enabled hunt pilot call, that agent will be logged off of the hunt group and will not receive additional hunt pilot calls unless he presses the "HLOG" soft key on the phone to log into the hunt pilot. This behavior is not configurable in Unified Communications Manager 9.0(1). In Unified Communications Manager 9.1(1), the administrator can choose whether hunt members remain logged in if the call is not answered. For more information, refer to "Automatically Logout Hunt Member on No Answer" in the *Cisco Unified Communications Manager Administration Guide*, and to "Call Queuing" in the *Cisco Unified Communications Manager Features and Services Guide*.

Paging

Now included with Unified Communications Manager is the Singlewire InformaCast product that provides paging capabilities for users to make point-to-point, or group pages, to and from Cisco IP Phones. The software and documentation for the InformaCast product is on a separate DVD included with the purchase of Unified Communications Manager. It is also available online as a software download on cisco.com.

The InformaCast product is divided into two categories, basic and advanced functionality. The basic paging features allow paging between Cisco IP Phones to groups and zones that the administrator configures. An unlimited number of groups is possible but with a maximum of 50 users total in each group in basic paging. Basic paging is provided as a new Unified Communications Manager feature at no cost. If there is a requirement for more than 50 users in a single group or for higher level capabilities, the advanced features of InformaCast are required and are highly recommended.

The advanced features of InformaCast include:

- Paging and Emergency Notification to All Users
- Paging to Overhead Analog and IP Speakers
- Bell Scheduling
- Prioritizing Emergency Notifications with Call Barge Option
- Pre-Recorded and Text only pages
- Integration with Social Media Sites for Notification
- Email and SMS Mass Notification
- Call Number Monitoring - 911 Alerting
- Integration with Jabber clients

There are numerous additional features of Advanced Paging. To determine if Advanced Paging/Notification is appropriate for the end user's Unified Communications Manager deployment, there is a 60 day trial of the advanced functionality to evaluate the higher level features. After installation of the software, there is an option to begin the demonstration period for full access to all capabilities. To retain Advanced Functionality after trial or if this functionality is required at the time of the Unified Communications Manager purchase, the Advanced Paging/Notification functionality can be purchased as a perpetual license from SolutionsPlus or as a subscription directly from Singlewire. For more information on the product's capabilities or for sales questions, contact Singlewire or refer to the documentation and support information included with the product.

Cisco Jabber Support for Single Sign-On

IM and Presence Release 9.1(1) supports Single Sign-On (SSO) for Cisco Jabber. The Cisco Client Profile Agent service is required for this feature. For more information, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager* or the *Cisco Unified Communications Operating System Administration Guide*.

Enhanced IM and Presence Deployment Support

It is no longer required that the enterprise-wide presence domain aligns with the DNS domain of any server. An IM and Presence deployment can have a common presence domain, while having nodes deployed across multiple DNS domains. If any IM and Presence node name is based on the hostname only, then all IM and Presence nodes must share the same DNS domain. However, if all IM and Presence nodes within the deployment have a node name set to that node's Fully Qualified Domain Name (FQDN) or IP Address, the following deployment options are supported.

- IM and Presence clusters deployed in different DNS domain or subdomains
- IM and Presence nodes within a cluster deployed within different DNS domains or subdomains
- IM and Presence nodes within a cluster deployed in a DNS domain that is different to the associated Cisco Unified Communications Manager cluster

For more information see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager* .

Partitioned Intradomain Federation with Microsoft Lync

The IM and Presence Service Release 9.1(1) supports Partitioned Intradomain Federation with Microsoft Lync. For more information see *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager* .

Licensing

Advanced UCL and UWL Premium license types are no longer applicable. The following device types, previously under Advanced UCL and UWL Premium, now require the Enhanced License type:

- Cisco IP Communicator

- Cisco Unified Personal Communicator
- Carrier-Integrated Mobile
- Unified Client Services Framework
- Cisco Telepresence EX60
- Cisco Telepresence EX90
- Cisco Dual Mode for Android
- Cisco Dual Mode for iPhone
- Cisco Unified Mobile Communicator
- IMS-integrated Mobile

Enhanced Plus UCL has been added, which includes the same device types and features as the Enhanced License type, and allows for up to 2 devices per user.

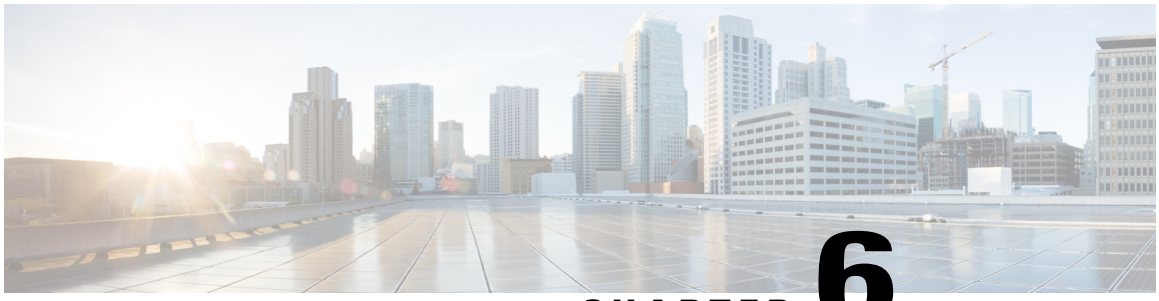
Cisco Unified Workspace License (UWL) Standard allows for up to 10 devices per user.

Customers who upgrade to Unified Communications Manager Release 9.1(1) from Release 9.0(1) must update their license file. Customers were issued Unified Communications Manager UWL Premium licenses for Enhanced, Enhanced Plus and UWL Standard in order to provide Jabber for Mobile and Jabber for Desktop clients in the Release 9.0(1) release. These licenses were installed and recognized on Enterprise License Manager Release 9.0(1) as UWL Premium.

In addition, license migration requests for upgrades to Release 9.0(1) included fulfillments of Advanced UCL licenses. However, when a Release 9.0(1) system is upgraded to Release 9.1(1) the licenses for Advanced and UWL Premium will no longer be valid. Customers that have UWL Premium or Advanced UCL licenses on their 9.0(1) system must upgrade Enterprise License Manager to Release 9.1(1) and submit their Release 9.0(1) license file to Cisco for conversion to Release 9.1(1) licenses. The conversion to Release 9.1(1) licenses will restore the original entitlements for Enhanced, Enhanced Plus and UWL Standard licenses. If your license file includes UWL Premium or Advanced UCL, contact Cisco at uc91-license@cisco.com for license file replacement.

Once a customer upgrades Unified Communications Manager to Release 9.1(1) from Release 9.0(1), they must upgrade Enterprise License Manager to Release 9.1(1) as well. Enterprise License Manager Release 9.0(1) will not recognize Unified Communications Manager Release 9.1(1) license requirements.

For more information, see the "Licensing" chapter of the *Cisco Unified Communications Manager Features and Services Guide*.



CHAPTER 6

Caveats

- Bug Search Tool, page 39
- Resolved Caveats, page 40
- Open Caveats, page 40

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 problems by using the Cisco Bug Search tool.

To access Bug Search, you need the following items:

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

Follow these steps to use Bug Search:

1. Access Bug Search: https://tools.cisco.com/bugsearch/.
2. Log in with your Cisco.com user ID and password.
3. If you are looking for information about a specific problem, enter the bug ID number in the **Search for:** field, and click **Go**.

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

Resolved Caveats

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

Tip

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

Related Topics

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

Open Caveats

The following sections describe possible unexpected behaviors in Unified Communications Manager Release 9.1(1) and IM and Presence Service Release 9.1(1):

- Open Caveats for Unified Communications Manager Release 9.1(1), on page 41
- Open Caveats for IM and Presence Service Release 9.1(1), on page 45
- Open Caveats for Enterprise License Manager 9.1(1), on page 47

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 Communications Manager Release 9.1(1), on page 41 and Open Caveats for IM and Presence Service Release 9.1(1), on page 45 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 39.

Open Caveats for Unified Communications Manager Release 9.1(1)

The following table lists open caveats which may cause unexpected behavior in Unified Communications Manager 9.1(1).

Table 5: Open Caveats for Unified Communications Manager

Identifier	Severity	Component	Headline
CSCuc25464	3	axl	GetPhone AXL responses seem slower in CUCM 9.0
CSCud36245	3	axl	CUCM Location Overwritten by CUCDM/VOSS modification - Refer: CSCuc36584
CSCud53481	3	axl	Add ServiceProfile is getting failed
CSCud68560	3	axl	Transfer-Encoding: chunked Protocol In Betz
CSCud10175	3	backup-restore	DRS screen does not work on Chrome Mac
CSCud33840	3	backup-restore	DRS backup failure shows incorrect information about features backed up
CSCua19534	3	bps-bat	BAT can't insert 10K remote destinations

Identifier	Severity	Component	Headline
CSCud16484	3	bps-import-export	BAT Import of Unassigned DN doesn't import CFA Dest, CFURExt VM checkbox
CSCtr14518	3	ccmcip	SRB:79XX, 99XX: Corporate Directory is displaying in English
CSCud13922	3	ccm-serviceability	RTMT reason code not proper when RT phones initiates energywise mode
CSCud67438	3	ccm-serviceability	Unified Serviceability Tools can not connect to other nodes
CSCud72605	3	ccm-serviceability	CCM raises SIPTrunkOOS alarm without any details
CSCty02858	3	cmcti	Get platform exception on transfer with multiple hold and resume
CSCuc70031	3	cmcti	ProviderOpen Request fail: core file generated
CSCuc76289	3	cmcti	Consult call hit platform exception
CSCuc97126	3	cmcti	CTIRD to release the shared line initiated call in LmKeySetupReq
CSCud17020	3	cmcti	Unable to update MGCP gateway page
CSCtk12124	3	cmui	Unable to update MGCP gateway page
CSCuc87927	3	cmui	EUPLA URI Format
CSCud21579	3	cmui	UOP - Multiple issues with ring settings parameters
CSCud42719	3	cmui	Directory Number configuration shows settings from previous dn config
CSCud59409	3	cmui	Logon status showing wrongly
CSCud05776	3	cp-device-manager	remote device remain unregistered after changing device pool
CSCud26795	3	cp-h323	CallerID not being shown when Caller ID received in facility msg
CSCud44041	3	cp-huntlist	Call Failure and Process leak for mobile calls for DVO-R calls over RL
CSCuc72096	3	cpi-appinstall	After fresh install show version inactive shows version of 0.0.0.0000-00
CSCud68399	3	cpi-appinstall	MCS7825H3- Upgrade failure in post-install phase boots to newer version
CSCud70135	3	cpi-appinstall	7.1.5 upgrade fail due to permissions issue on /common/download

Identifier	Severity	Component	Headline
CSCud49047	3	cpi-cert-mgmt	RTMT Option To Download Certificate Change Notification Service Logs
CSCud41456	3	cpi-os	Not able to login to tty console when sub is isolated from cluster
CSCua84906	3	cpi-os	SSL/TLS Protocol Information Disclosure (CVE-2011-3389)
CSCuc76911	3	cpi-os	L2 upgrade through local source fails
CSCud59239	3	cpi-os	CUCM Replication setup cdr define fails with error 5 delaying setup
CSCud43906	3	cpi-security	NIC Teaming has ICMP echo reply blocked with Asymmetric routing
CSCud71104	3	cpi-security	DRS Restore Fails when FIPS is enabled
CSCud69213	3	cpi-security	DRS Restore Fail for Fips enabled
CSCuc19625	3	cp-mediacontrol	CUCM Responds to 200 OK with mid-call Invite without SDP
CSCuc94411	3	cp-mediacontrol	Incorrect comparison for process name
CSCud18762	3	cp-mediacontrol	Does not get audio RSVP reservation for AAC in video call
CSCud30136	3	cp-mediacontrol	Conf reconnect between SIPv6 w/o MTP and SIPv6 w MTP SIP ICT fails
CSCud38314	3	cp-mediacontrol	CUCM disconnects call when the ISDN Gateway REINVITES and adds content
CSCud59919	3	cp-mediacontrol	Phone1 drops out of conference call once conference is setup
CSCuc83668	3	cp-mobility	SNR will not handle overlap receiving from QSig MGCP Gateway
CSCud66384	3	cp-qsig	QSIG Path replacement fails after CUCM detects collision
CSCud59803	3	cp-sip-station	No announcement when DVOR to an invalid number over SIP trunk
CSCud61819	3	cp-sip-station	Placed calls incorrect when using overlap receiving
CSCuc80321	3	cp-sip-trunk	SIP OOB-RFC2833 DTMF fails if early offer is used with "No Preference"
CSCuc80699	3	cp-sip-trunk	[SX20]CUCM-VCS[Edge95-H323] calls disconnects when SX20 has no H.261

Identifier	Severity	Component	Headline
CSCud22722	3	cp-sip-trunk	CTS Endpoint calls into Telepresence Server fail when BFCP is enabled
CSCud38739	3	cp-sip-trunk	No video on H323 endpoints when vcs-interop script enabled on Conductor
CSCud48539	3	cp-sip-trunk	VCS-CUCM interworking call failure
CSCud64851	3	cp-sip-trunk	CM does not send 200 OK due to glare before call is answered.
CSCud73145	3	cp-sip-trunk	Random overwrite of memory in CallManager/Source/ProcessSIPHandler.cpp
CSCuc89953	3	cp-supplementary-services	SIP MCU Conference unregisters from CUCM after two resets
CSCud52162	3	cuc-tomcat	Tomcat FORM Auth and CRSF Guard Vuls (CVE-2012-3546,CVE-2012-4431)
CSCtz07814	3	database	dbmon monitoring needs to be ignored during replication set-up
CSCuc22587	3	database	CUCM DB Replication takes a long time to repair componentversion table
CSCuc47907	3	database	ULT fields not allowing URI format
CSCud29372	3	dial-num-analyser	Browser issue on Dialed Number Analyzer page
CSCud57102	3	dial-num-analyser	DNA does not properly use the device mobility CSS from device pool
CSCud21371	3	elm	JPN: ELM: Description of License is garbled in License
CSCud25936	3	elm	License install with cert should fail if the clock is way behind
CSCud68280	3	elm	Standalone ELM set network hostname command doesn't update DB properly
CSCud69222	3	elm	DRS Restore Fails when FIPS is enabled
CSCud51221	3	ext-mobility	EMServiceServelet doesn't accept special characters (<, &)
CSCud62438	3	ext-mobility	Randomly EM username not remembered (Remember the Last User Logged true)
CSCsy73190	3	ipma-service	Unable to change the default assistant from Manager UI and Assistant con
CSCuc84064	3	jtapisdk	Get post condition fail on connect to prefixDpark

Identifier	Severity	Component	Headline
CSCud12752	3	jtapisdk	Get party info length incorrect after drop shareline from conference
CSCud15589	3	jtapisdk	Get wrong number of connection after transfer from remote device to HL
CSCud05621	3	rtmt	RTMT version 8.9X and 9.0 still reference the deprecated NetDump utility
CSCud22600	3	rtmt	Periodic RTMT 'Add Certificate to Store' pop-ups during normal operation
CSCud44059	3	rtmt	Session Trace cannot find SIP message when GZO file changes to GZ
CSCud12493	3	sch	Special char entry in Call Home page throw DB error
CSCuc85754	3	selinux	Identity change process intermittently fails due to hostname not updating
CSCud18819	3	serv-soap	Log collection SOAP API stops unexpectedly
CSCud13670	3	tapisdk	LINE_REMOVE event not returned on disabling SuperProvider at user admin
CSCud37116	3	tapisdk	dwParam2 (cause code) has changed in 9.0 causing compatability issue
CSCud23599	3	tftp	CSCtq39584 fix is failing to clear active connections
CSCud67624	3	ucm-user-licensing	TelePresence Room license requirements require additional Enhanced
CSCuc02731	3	uri-dialing	Some special character cannot be dialed from phone

Open Caveats for IM and Presence Service Release 9.1(1)

The caveats in the table which follows describe possible unexpected behavior in the latest IM and Presence Service release. These caveats may also be open in previous releases. Bugs are listed in alphabetical order by component and then in numerical order by severity.

Table 6: Open Caveats for IM and Presence Service Release 9.1(1)

Identifier	Severity	Component	Headline
CSCtw75780	3	bat	Some imported contacts' presence not showing when max contacts size set
CSCtz96671	3	cupxcpconfig	Incorrect restart notification for sub's XMPP fed connection manager
CSCuc76484	3	database	Exception thrown when executing "dbl sync -- updstat"
CSCud22574	3	epe	Out of memory on startup due to large number of WinfoEventTable entries
CSCua09500	3	epe	Presence engine hangs on startup
CSCua41574	3	epe	HA issue: users logging out on the sub when xcp router comes up on pub
CSCua60813	3	epe	Presence Engine core dump if IMDB services shut down on large system
CSCtz99702	3	epe	HA issue: users logging out on the sub when xcp router comes up on pub
CSCub30575	3	gui	JPN:CUP: OS Admin: Error occurs when opening HELP
CSCtr36119	3	gui-troubleshooter	Exchange Server Status reports false positives
CSCuc95669	3	security	IPSec cannot be set up because ipsec-truststore cannot accept leaf certs
CSCud22455	3	security	name can not be changed, it reports that the old password doesn't match
CSCtz25566	3	security	HA can't be enabled - version missing
CSCud51156	3	security	SUB upgrade fails with FIPS enabled
CSCud34859	3	selinux	Third Party LDAP Connection Troubleshooter test fails to run
CSCua57924	3	serviceability	Warn admin when taking critical services down with HA enabled
CSCub10356	3	serviceability	IM&P node cannot access / control a peer node's services on the GUI
CSCuc32578	3	serviceability	Most the services holding to STARTING state for long time
CSCtn62906	4	database	Incorrect destination ports for MER after upgrade 7.X -> 8.X

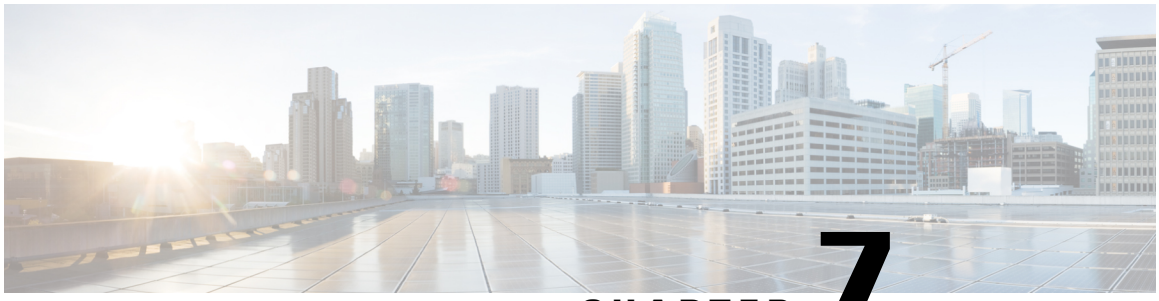
Identifier	Severity	Component	Headline
CSCud00064	4	gui-admin	CM Presence Gateway can't be configured using DNS SRV FQDN
CSCtj69153	5	gui-admin	CM Presence Gateway can't be configured using DNS SRV FQDN
CSCua68248	6	epe	Add NTLMv2 support to CUP Exchange Calendaring
CSCtr42784	6	gui	Admin GUIs appear partially translated for unsupported locales

Open Caveats for Enterprise License Manager 9.1(1)

The caveats in the table which follows describe possible unexpected behavior in the latest Enterprise License Manager release. These caveats may also be open in previous releases.

Device	Description	Fix
License Migration Utility	• Supports license upgrades for Unified Communication Manager versions 6.X to 8.X • Uninstalled DLUs and unregistered license PAKs must be fulfilled and installed prior to Unified Communication Manager upgrade • Migration to 9.1(1) through 9.0(1) may result in a license upgrade failure • Installing invalid licenses prior to upgrade to 9.1(1) may result in a license upgrade failure	• For Release 5.x and pre-Release 5.0 systems, submit a case to licensing@cisco.com • Uninstalled DLUs and unregistered PAKs cannot be installed onto Enterprise License Manager. Submit a case to licensing@cisco.com
Upgrades to Release 9.0(1) or Release 9.1(1).	Upgrade orders for Release 9.0(1) or Release 9.1(1) do not issue any license PAKs. License upgrades to Release 9.0(1) or Release 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 Release 9.0(1) or Release 9.1(1). From the Enterprise License Manager go to **License Management > License Planning > Upgrade Licenses**.

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



CHAPTER 7

Documentation Updates

- License Mac References, page 50
- Administration Guide, page 50
- Bulk Administration Guide, page 54
- Call Detail Records Administration Guide, page 55
- Changing IP Address and Hostname, page 59
- CLI Reference Guide, page 61
- Deployment Guide for IM and Presence Service, page 62
- Disaster Recovery System Guide, page 63
- Features and Services Guide, page 65
- IM and Presence Administration Online Help, page 74
- Installing Cisco Unified Communications Manager, page 75
- Interdomain Federation for IM and Presence Service, page 76
- Managed Services Guide, page 77
- Migration and Upgrade Guide, page 78
- OS Administration Guide, page 78
- Partitioned Intradomain Federation for IM and Presence Service, page 79
- Real-Time Monitoring Tool Guide, page 79
- Security Guide, page 83
- Serviceability Guide, page 86
- System Guide, page 87
- TCP and UDP Port Usage Guide, page 97
- User Options Guide, page 98
- Upgrade Guide, page 98
- XML Developers Guide, page 100

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.

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.

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.

CTI Remote Device Name Cannot Contain Spaces

This documentation update resolve CSCue57419.

In the CTI remote device configuration settings window, you cannot add a space in the Device name field for CTI remote devices.

Directory Number Line Behavior in Cisco Unified Communications Manager

This documentation update resolves CSCuo74599.

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

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

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

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.

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.

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.

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.

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".

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.

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.

Bulk Administration Guide

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
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

Field Names	Recorded Call CDR	Recording Call CDR1	Recording Call CDR2
origCalledPartyRedirectReason	0	354	354
lastRedirectRedirectOnBehalfOf	0	354	354
origCalledPartyRedirectOnBehalfOf		27	27
lastRedirectRedirectOnBehalfOf		27	27
origConversationID	0	16777111	16777111

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

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

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 " "

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
```

Database Replication After Hostname Change

This documentation update resolves CSCug77319.

After you change the hostname of a Unified Communications Manager publisher or subscriber node, you must run a CLI command to set up database replication across the cluster.

From the publisher server, run utils dbreplication rebuild all to set up replication across the whole cluster again.

Do Not Change the Hostname and IP Address Together

This documentation update resolves CSCug52160.

You may need to change the IP address or hostname on a Cisco Unified Communications Manager server. For example, you may need to move the server from one segment to another or to resolve a duplicate IP address problem.

If you change the IP address or the hostname of a server in a Cisco Unified Communications Manager cluster, ensure that you do not change both the IP address and the hostname at the same time. If you change both settings at the same time, the Cisco Unified Communications Manager database becomes inaccessible.

Error in the Procedure for Changing the Hostname

This documentation update resolves CSCug89794.

In the document *Changing the IP Address and Hostname for Cisco Unified Communications Manager*, there is an error in the procedure "Changing the IP Address for Servers that are Defined by an IP Address."

When you change the hostname for servers that are defined by an IP address, you must run the following command after you have changed the hostname and the server has rebooted:

utils dbreplication dropadmindb

IP Address, Domain and Hostname for IM and Presence Service

The chapter titled “Modify the SIP Domain of an IM and Presence Cluster” has been removed and replaced with a new chapter titled “Modify Server Domain.” Minor updates have been made to the remaining chapters to include instructions for when the node name is a Fully Qualified Domain Name (FQDN).

set network ip eth0 Requires Gateway Parameter

This documentation update resolves CSCuh27880.

In the document *Changing the IP Address and Hostname for Cisco Unified Communications Manager*, there is an error in the procedure "Changing the IP Address for Servers that are Defined by an IP Address."

When you use a CLI command to change the IP address of the server, you must run the following command:

set network ip eth0 <*ip addr*> <*netmask*> <*gw*>, where <*ip_address*> specifies the new server IP address, <*netmask*> specifies the new server network mask, and <*gw*> specifies the default gateway.

CLI Reference Guide

Enable or Disable FIPS for IM and Presence Service

This documentation update resolves CSCuo56537.

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

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

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.

run cuc sysagent task Example is Incorrect

This documentation update resolves CSCum43072.

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.

set network domain Conflicting Information

This documentation update resolves CSCup03425.

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

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

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

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

Show perf query counter Command Output

This documentation update resolves CSCuo70238.

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

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

Deployment Guide for IM and Presence Service

Enhanced IM and Presence Deployment Support

The procedure to configure XMPP certificate settings has been removed from the “Security configuration on IM and Presence” chapter.

The following topics have been added to support the Enhanced IM and Presence Deployment Support feature:

- DNS domain configuration
- Presence domain configuration
- Specify DNS domain associated with Cisco Unified Communications Manager cluster

The following topics have been updated to support the Enhanced IM and Presence Deployment Support feature:

- Node name recommendations
- Node name value for intercluster deployments
- Presence domain value for intercluster deployments

The topic titled "Single Sign-On setup" has been updated to include support for the Cisco Client Profile Agent. This service is required for Cisco Jabber Single Sign-On (SSO) support.

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 the Bulk Administration Tool; 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.

Locale Installation Information Update

This documentation update resolves CSCue81331.

Removed the procedure to install Locale installer on Cisco Unified Communications Manager with instructions to see the *Upgrade Guide for Cisco Unified Communications Manager* for details about installing locales on the Cisco Unified Communications Manager.

Additional topics from the *Upgrade Guide for Cisco Unified Communications Manager* were added that cover the following:

- Locale installation considerations and information to obtain the Locale Installer from www.cisco.com.
- Locale file descriptions for Cisco Unified Communications Manager (cm-locale-language-country-version.cop), the Cisco Unified Communications Manager combined network locale file (cm-locale-combinednetworklocale-version.cop), and for IM and Presence Service (ps-locale-language_country-version.cop).

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

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 Group Visual Notification Does Not Support Localization

This documentation bug resolves CSCup04321.

Localization support is not available for call pickup group visual notification, because this notification uses ASCII for the alerting name.

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.

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*.

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.

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

EMCC Incorrect Limitation

This documentation update resolves CSCum74529.

The following Extension Mobility Cross Cluster limitation is incorrect:

“ Duplicate user ID does not get supported (for either the same or different PIN), because the behavior is unpredictable.”

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**.

EMCC Video Calling Override Common Settings

This documentation update resolves CSCue66051.

In the chapter “Extension Mobility Cross cluster,” Step 12 of Configure EMCC reads as follows:

In either window, set the Video Capabilities drop-down list box as Enabled. (This setting may be enabled by default per cluster.)

This is incorrect. the corrected text is as follows:

In either window, set the Video Capabilities drop-down list box as Enabled and check the Override Common Settings check box. (Although this setting may be enabled by default per cluster, it may be necessary to check the Override Common Settings check box and save the change)

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.

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.

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 Now Supports Device Owners

This documentation update resolves CSCun04965.

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

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.

Jabber Devices Count as Registered Devices

This documentation update resolves CSCur73944.

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

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

Licensing Usage Report Correction

This documentation update resolves CSCud80834.

The license type list in the "Licensing" chapter contains an incomplete list. The following is the corrected list:

System > **Licensing** > **License Usage Report**	This window displays the current license usage on the system. The License Type column lists the various types of licenses: • Essential • Basic • Enhanced • Advanced • Premium • Professional • TelePresence Room

Locale Usage for Queue Announcements Clarification

This documentation update resolves CSCuj05744.

The following content is omitted from the Announcement Settings table in the Music On Hold chapter.

- Periodic Announcement: MOH server always plays the periodic announcement regardless of other settings.
- Initial announcements : Initial announcements are always simulcast to each new caller. Periodic announcements are multicast to queued callers at the specified time interval. Callers who join the queue after the periodic announcement has begun to play may only hear a portion of the announcement.
- Locale Announcement :
  - Prompts played by MOH will use the setting for Locale Announcement.
  - Prompts played by ANN will use the User Locale of the calling party.

MGCP FXS Ports Do Not Require a License

This documentation update resolves CSCum47807.

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

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

Music On Hold and Native Call Queuing Behavior

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

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

Native Call Queuing Periodic Announcement Behavior

This documentation update resolves CSCui20806.

The following information is omitted from the "Call Queuing" and "Music On Hold" chapters in the *Features and Services Guide*:

Initial announcements are always simulcast to each new caller. Periodic announcements are multicast to queued callers at the specified time interval. Callers who join the queue after the periodic announcement begins to play may only hear a portion of the announcement.

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.

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.

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.

IM and Presence Administration Online Help

Microsoft Lync and FQDN Updates

The following updates were made to the Cisco Unified CM IM and Presence Administration Online Help:

- The Cluster Topology configuration topic has been updated to recommend that you specify the FQDN as the node name.
- Minor changes to the following topics to include support for Microsoft Lync:
  - Bulk Administration Tool Configuration to Update Users' Contact Lists
  - Bulk Administration Tool Configuration to Upload and Download Files
  - Certificate Import Tool Configuration
  - IM and Presence Configuration
  - Microsoft RCC Troubleshooter Configuration

Extension Mobility Now Supports Device Owners

This documentation update resolves CSCun04965.

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

XMPP Certificate Settings Section Missing

This documentation update resolves CSCue50920.

The XMPP Certification Settings content was removed in error from the Security Configuration topic. The information that was removed is contained in the following table.

XMPP Certificate Settings
Domain Name for XMPP Server-to-Server Certificate Subject Common name Enter a server-to-server domain name for this cluster. If you change this domain name value, you must regenerate affected XMPP S2S certificates before you restart the Cisco XCP Router service. The entry that you configure here will be visible on the associated XMPP certificates after you regenerate the certificates. **Allowed Values**: Alphanumeric (a-zA-Z), period (.), and dash (-), and asterisk (*). **Example:** Domain: cisco.com

XMPP Certificate Settings
Use Domain Name for XMPP Certificate Subject Common Name **Default Setting**: Off Check this check box if you want the general XMPP certificate to use the same domain name as the XMPP server-to-server certificate. If you change this setting, you must regenerate the XMPP certificate before you restart the Cisco XCP Router service.

Installing Cisco Unified Communications Manager

Add a New Node to an Existing Cluster

The procedure “Add a new node to an existing cluster” has been updated to indicate that after you install a new node in an existing cluster, all phones that are registered to the cluster are reset.

Change the IM and Presence Node Name

The procedure to change the IM and Presence node name to a resolvable value has been updated to specify that for non-DNS deployments you must change the IM and Presence node name to be the server's IP address after installation is complete.

External NTP Server Requirements

The procedure “Set up first node” has been updated to remove the requirement that the external NTP server be Stratum 5 or higher. When you configure the first node, Cisco recommends configuring the publisher to point to a Stratum 1, Stratum 2, or Stratum 3 NTP server to ensure that the cluster time is synchronized with an external time source.

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*.

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.

Microsoft Lync Support

IM and Presence Service Release 9.1(1) supports Partitioned Intradomain Federation with Microsoft Lync. A new chapter titled *Configuration of Microsoft Lync for Partitioned Intradomain Federation* has been added. Several updates have also been made to other chapters to support Microsoft Lync.

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

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

Migration and Upgrade Guide

Server Support

This document contains information about the supported paths for direct upgrades. The section “Server support for direct to Release 9.0 upgrade path,” incorrectly refers to Release 9.0; it should refer to Release 9.x.

OS Administration Guide

Client Profile Agent Update

The chapter “Single Sign-On” has been updated to include the Cisco Client Profile Agent. This service is required for Cisco Jabber support for Single Sign-On (SSO).

Documentation Update for Certificate Monitor Configuration

This documentation update resolves CSCuo30610.

The following information is omitted from the Certificate Monitor Field Descriptions table:

You can enter multiple email addresses by separating the email addresses with a semicolon (;). Do not insert a space between the email addresses. For example, test@cisco.com;test1@cisco.com;test2@cisco.com, and so on.

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.

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

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).

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 9: 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%)

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.

Counters	Counter Description
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.
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.

An RTMT Update Is Required When You Upgrade Unified CM

This documentation update resolves CSCul38276.

When you perform an upgrade to Unified Communications Manager, you must also upgrade the Cisco Unified Real Time Monitoring Tool (Unified RTMT).

Upgrade RTMT

Tip To ensure compatibility, Cisco recommends that you upgrade RTMT after you complete the Cisco Unified Communications Manager upgrade on all servers in the cluster.

RTMT saves user preferences and downloaded module jar files locally on the client machine. The system saves user-created profiles in the database, so you can access these items in Unified RTMT after you upgrade the tool.

Before You Begin

Before you upgrade to a newer version of RTMT, Cisco recommends that you uninstall the previous version.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Application** > **Plugins**.

Step 2 Click **Find**.

Step 3 Perform one of the following actions:

- To install the tool on a computer that is running the Microsoft Windows operating system, click the **Download** link for the Cisco Unified Real-Time Monitoring Tool - Windows.
- To install the tool on a computer that is running the Linux operating system, click the **Download** link for the Cisco Unified Real-Time Monitoring Tool - Linux.

Step 4 Download the installation file to your preferred location.

Step 5 Locate and run the installation file.
The extraction process begins.

Step 6 In the RTMT welcome window, click **Next**.

Step 7 Because you cannot change the installation location for upgrades, click **Next**.
The Setup Status window appears; do not click Cancel.

Step 8 In the **Maintenance Complete** window, click **Finish**.

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.

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 Can 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 causes an automatic restart of the phones on the cluster on which you imported the certificates.

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".

Serviceability Guide

AXL Web Service Requirement for ICSA HA

This documentation update resolves CSCup00956.

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

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

Cisco CAR DB Service

This documentation update resolves CSCup98304.

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

Cisco CAR DB Service

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

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

Cisco 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).

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.

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.

System Guide

Configure LDAP Directory

The Configure LDAP Directory topic in the "Directory Overview" chapter contains an out-of-date list of supported directories. The list incorrectly states that Cisco Unified Communications Manager supports Microsoft Active Directory 2000 and iPlanet Directory Server 5.1. In addition, the list omits Sun One Directory Server 7.0 and Oracle Directory Server Enterprise Edition 11gR1, both of which Cisco Unified Communications Manager supports, from the list of supported directories.

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.

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

Phones That Support Private Line Automatic Ringdown

This documentation update resolves CSCuf16795.

The Private Line Automatic Ringdown (PLAR) topic in the “Dial Rules Overview” chapter incorrectly states that only Cisco Unified IP Phones 7940/41, 7960/61, and 7970/71 support PLAR for SIP. However, the following Cisco Unified IP Phones also support PLAR over SIP: 9971, 9951, 8961, and Cisco ATA 187.

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.

TFTP Cisco SIP Phones

This documentation update resolves CSCud67724.

The "Configure TFTP for Cisco Unified IP phones that run SIP" topic contains an out-of-date table that lists the configuration files that are generated based on the type of phone that is running SIP. The table is missing several Cisco Unified IP Phones. The following is the updated table:

Model	SIP IP Phone	Dial Plan	Softkey Template
9971, 9951, 8961, 8945, 8941, 7975, 7971, 7970, 7961, 7941, 7911, Cisco Cius	SEP<mac>.cnf.xml	DR<dialplan>.xml	SK<softkey_template>.xml
Cisco TP 1000, Cisco TP 1100, Cisco TP 1300-47, Cisco TP 1300-65, Cisco TP 1310-65			
7960, 7940	SIP<mac>.cnf	<dialplan>.xml	Not configurable
7905	Id<mac>	Parameter in Id<mac>	Not configurable
7912	gk<mac>	Parameter in gk<mac>	Not configurable
Cisco IP Communicator	<Device Name>.cnf.xml	Parameter in <Device Name>.cnf.xml	Parameter in <Device Name>.cnf.xml
Cisco Jabber for Tablet	TAB<Userid in Upper Case>.cnf.xml	Not configurable	SK<softkey_template>.xml

Updates to Supported Cisco Unified IP Phones

This documentation update resolves CSCue50755.

The Supported Cisco Unified IP Phones topic omits the following supported phones.

Note Phone models that are End of Software Maintenance will continue to be supported on the latest Unified Communications Manager releases, but they will not take advantage of any new Unified Communications Manager features or firmware features associated with that release. For more information on End of Sale phone models, reference the End of Sale announcement for that model for information on level of firmware and hardware support.

Cisco Unified IP Phone Model	Description
Cisco Unified IP Phone 8945	The Cisco Unified IP Phone 8945 delivers affordable, business-grade voice and video communication services to customers worldwide. The Cisco Unified IP Phone 8945 has the following features: • The phone delivers VGA presentation for calling, video calling, and applications, in addition to a 5-inch (10-cm) graphical TFT color display, 16-bit color depth, 640 x 480 effective pixel resolution, and backlighting. The display also supports localization requiring double-byte Unicode encoding for fonts • The phone supports four lines and four context-sensitive soft keys along with a high-definition voice, full-duplex speakerphone for a more productive and more flexible endpoint experience • Fixed keys for hold, transfer, redial, and conference; a tri-color LED line; and feature keys also make the endpoint simpler and easier to use. • The Cisco Unified IP Phone 8945 supports right-to-left language presentation on its display, addressing the language localization needs of global customers. Cisco Unified IP Phone 8941 supports SCCP and SIP.

Cisco Unified IP Phone Model	Description
Cisco Unified IP Phone 8941	The Cisco Unified IP Phone 8941 delivers affordable, business-grade voice and video communication services to customers worldwide. The Cisco Unified IP Phone 8941 has the following features: • The phone delivers VGA presentation for calling, video calling, and applications, in addition to a 5-inch (10-cm) graphical TFT color display, 16-bit color depth, 640 x 480 effective pixel resolution, and backlighting. The display also supports localization requiring double-byte Unicode encoding for fonts • The phone supports four lines and four context-sensitive soft keys along with a high-definition voice, full-duplex speakerphone for a more productive and more flexible endpoint experience • Fixed keys for hold, transfer, redial, and conference; a tri-color LED line; and feature keys also make the endpoint simpler and easier to use. • The Cisco Unified IP Phone 8941 supports right-to-left language presentation on its display, addressing the language localization needs of global customers. Cisco Unified IP Phone 8945 supports SCCP and SIP.

Cisco Unified IP Phone Model	Description
Cisco Unified IP Phone 7961G-GE	The new Cisco Unified IP Phone 7961G-GE delivers the latest technology and advancements in Gigabit Ethernet IP telephony. This phone not only offers enhanced functionality for managers that require advanced communications capabilities, it also brings network data and applications to users quickly with its Gigabit Ethernet port for integration to a PC or desktop server. The Cisco Unified IP Phone 7961G-GE is standards-based to deliver better interoperability and greater deployment flexibility. This state-of-the-art Gigabit Ethernet IP phone also offers the same features as the Cisco Unified IP Phone 7961G, including: • High-resolution, graphical 4-bit grayscale display (320 x 222) that supports double-byte characters and Unicode text to benefit Extensible Markup Language (XML) application developers [Note: This phone requires IEEE 802.3af inline power or the use of a local power cube] • A full-featured handset with six programmable line and feature buttons • Four interactive softkeys to help guide users through various call features and functions

Cisco Unified IP Phone Model	Description
Cisco Unified IP Phone 7941G	The new Cisco Unified IP Phone 7941G-GE delivers the latest technology and advancements in Gigabit Ethernet IP telephony. This phone not only offers enhanced functionality for businesses that require advanced communications capabilities, but also brings network data and applications to users quickly with its Gigabit Ethernet port for integration to a PC or desktop server. The Cisco Unified IP Phone 7941G-GE is standards-based to deliver better interoperability and greater deployment flexibility. This state-of-the-art Gigabit Ethernet IP phone offers the same features as the Cisco Unified IP Phone 7941G and includes: • High-resolution, graphical 4-bit grayscale display (320 x 222) that supports double-byte characters and Unicode text to benefit Extensible Markup Language (XML) application developers [Note: This phone requires IEEE 802.3af inline power or the use of a local power cube] • A full-featured handset that provides two programmable line and feature buttons • Four interactive softkeys to help guide users through various call features and functions
Cisco Unified IP Phone 7926G	Increase the responsiveness of your mobile workforce within the campus and reduce overall costs with the Cisco Unified Wireless IP Phone 7926G. This portable, wireless IP phone delivers Cisco Unified Communications, integrated bar-code scanning, and custom applications. Building on the capabilities of the Cisco Unified Wireless IP Phone, the 7926G includes: • Integrated EA11 2D bar-code scanner to track location, progress, and inventory • Ability to decode bar code symbologies; configure with Cisco Unified Communications Manager • Mobile Information Device Profile custom applications (MIDlets) for faster response • Specially designed holster and leather case

Cisco Unified IP Phone Model	Description
Cisco Unified Wireless IP Phone 7925G EX	The Cisco Unified Wireless IP Phone 7925G-EX delivers all of the capabilities of the Cisco Unified Wireless IP Phone 7925G with the ruggedness and resiliency that is certified for deployment in potentially explosive environments such as chemical and manufacturing plants, utilities, and oil refineries. Features include: • Atmospheres Explosibles (ATEX) Zone 2/Class 22 and Canadian Standards Association (CSA) Class I Division II certifications • IP64 rating for superior dust resistance with splashing water resistance adds resiliency. • Industry-standard yellow styling offers fast recognition in event of an emergency. • 802.11a/b/g standards for voice over WLAN (VoWLAN) communications support. • Supports third-party Bluetooth 2.0 headsets for added freedom • Large 2-inch color (176 x 220 pixel) display makes viewing easy. • Exceptional voice quality with high-definition voice (HD voice) • Built-in full-duplex speakerphone for high-quality hands-free communications. • Applications key provides direct access to XML applications such as push-to-talk and Lone Worker. • Extended-life batteries deliver a minimum of 13 hours talk time and up to 240 hours standby

Cisco Unified IP Phone Model	Description
Cisco Unified SIP Phone 3911	The Cisco Unified SIP Phone 3911 is a cost-effective, entry-level phone that addresses the needs of a lobby, laboratory, manufacturing floor, or hallway. This single-line phone with speakerphone and internal microphone can also fill the communication needs of cubicle, retail, classroom, or manufacturing workers or anyone with low to moderate telephone needs. The Cisco Unified SIP Phone 3911 provides: • Fixed feature keys that provide one-touch access to redial, transfer, conference, hold, line select, mute, speakerphone, and voicemail access features • A display that supports additional capabilities such as caller ID, call history, and phone configuration • Choice of IEEE 802.3af Power over Ethernet (PoE) or local power through an optional power adaptor
Cisco Unified SIP Phone 3905	Replace your existing analog and digital phone deployments with affordable IP communication endpoints using the Cisco Unified SIP Phone 3905. This phone also gives you access to the comprehensive suite of capabilities supported by Cisco Unified Communications Manager. The Cisco Unified SIP Phone 3905 includes interactive features such as: • Single-line IP phone with support for up to two concurrent calls • Graphical 128x32-pixel monochrome display with a two-way navigation button • Full duplex speakerphone for flexibility with hands-free communications • Fixed keys for common telephony features: hold, redial, transfer, and mute • Foldable, single-position display stand to simplify wall-mount deployments

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.

TCP and UDP Port Usage Guide

Destination Listener port value for IM and Presence

In the section titled "Port Usage Information for the IM and Presence Service", the table listing the IM and Presence Service Ports for Presence Engine Requests was updated. The TCP/UDP Destination Listener port value for IM and Presence was updated to port 5080 as follows:

Table 10: IM and Presence Service Release 9.x Ports - Presence Engine Requests

From (Sender)	To (Listener)	Protocol	Transport Protocol	Destination/ Listener	Source/ Sender	Remarks
IM and Presence	IM and Presence (Presence Engine)	SIP	UDP/TCP	5080	Ephemeral	Default SIP UDP/TCP Listener port

Ports Between Unified CM and LDAP

This documentation update resolves CSCul08363.

This guide lists the destination port from Unified Communications Manager to External Directory as Ephemeral.

Unified Communications Manager to External Directory is 389 LDAP, 636 for secure LDAP, or 3269 for global catalog. External Directory to Unified Communications Manager is Ephermeral.

The following table shows the correct ports between Unified Communications Manager and LDAP directory.

Table 11: Ports Between Cisco Unified Communications Manager and LDAP Directory

From (Sender)	To (Listener)	Destination Port	Purpose
Unified Communications Manager	External Directory	389, 636, 3628, 3629 / TCP	Lightweight Directory Access Protocol (LDAP) query to external directory (Active Directory, Netscape Directory)
External Directory	Unified Communications Manager	Ephemeral	

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

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.

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.

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.

XML Developers Guide

CSCup71020 MaxReturnedDevices in Serviceability XML

The *Cisco Unified Communications Manager XML Developers Guide, Release 9.1(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.