Release Notes for Cisco Unified Communications Manager, Release 9.1(2)

First Published: 2013-06-24

Last Modified: 2014-02-14

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

Text Part Number: OL-29587-01

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

© 2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Introduction** 1

About Release Notes 1

Hardware Server Requirements 2

Server software requirements 4

Supported browsers 4

CHAPTER 2 **Unified Communications Manager Upgrade to Release 9.1(2)** 5

Software Version Number 5

Pre-Upgrade Tasks 5

Overview of Software Upgrade Process 8

Upgrade on Virtual Server 8

Configuration Changes During Upgrade 9

Supported Upgrades 10

Upgrade File 10

Upgrade Media 10

Software Upgrade Procedures 11

Install the COP File 11

Upgrade to Restricted or Unrestricted Unified Communications Manager 11

Upgrade From a Local Source 11

Upgrade From a Remote Source 13

Supported SFTP Servers 13

Bridge Upgrade 15

Post-Upgrade Tasks 15

Latest Software and Firmware Upgrades 15

Firmware 15

Software 16

Related Documentation 16

Limitations and Restrictions 16

CHAPTER 3 IM and Presence Service Upgrade to Release 9.1(1a) 19

New system installation information 19

System Upgrade 19

Supported Upgrade Paths to IM and Presence Service Release 9.1(1a) 20

Upgrade from Cisco.com 20

Upgrade order 21

Software licensing requirements for VMware 21

Recommendations for Release 8.0(x), 8.5(x), or 8.6(x) to 9.1(1) Upgrades 21

OS Administrator Account Required for IM and Presence Upgrades 22

CHAPTER 4 Important Notes 23

60 GB 9.x UCM VM Deployed From OVA Has Unaligned Partitions 23

Bridge Upgrade Fails with Insufficient Disk Space 24

Call Forward Notification All Lines 24

Cannot Add Subscriber When Performing Cisco Business Edition 5000 to Cisco Business Edition 6000 Migration 25

Changed License Calculations for Extension Mobility 25

Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets 25

Cisco Unified Mobility Disclaimer 26

Configure LDAP Directory 26

Jabber Certificate Warnings with IM and Presence Service 26

Migrating Phones Between Clusters 27

Partition Alignment Check in VMware Installation CLI and GUI 27

Phone Support for URI Dialing Display Preference Service Parameter 28

Upgrade to 9.1(1) Fails with Insufficient Disk Space 28

Reduce Disk Space Utilization 28

Devices Reset while Certificate Regeneration 29

MGCP IOS Gateway From PSTN Does Not Support Connected Address in ISDN Notify 29

Perfect Forward Secrecy is not Supported in IPsec Configuration 29

Change Perfmon Counter File Size Parameters in RTMT 30

CHAPTER 5 New and Changed Information 31

Jump Upgrade 31

License Migration 32
Data Collection Before Upgrade 33
Planning Before Upgrade 34
Installation and Upgrade 35
Request Licenses 36
Deployment 36
New CLI Commands for Release 9.1(2) 36
iX Media Channel 37
Include Partition Alignment Check in VMware Installation CLI and GUI 37
V.110 (Clear Channel Codec) Enhancement to Support GSM Networks 38
Cisco Voice Gateways (ISR) 44XX Series 38
Cisco ISR44XX Series Gateways 38
Cisco Integrated Services Router 4451-X 39
Cisco Voice Gateways 39
Standalone Voice Gateways 40
Cisco VG310 Analog Phone Gateway 41
Cisco VG320 Analog Phone Gateway 41
Cisco VG350 Analog Phone Gateway 41
Voice Gateway Model Summary 41

CHAPTER 6 **Caveats 43**
Bug Search Tool 43
Resolved Caveats 44
Open Caveats 44
Open Caveats for Unified Communications Manager Release 9.1(2) 45
Open Caveats for IM and Presence Service Release 9.1(1a) 48
Open Caveats for Enterprise License Manager Release 9.1(2) 50

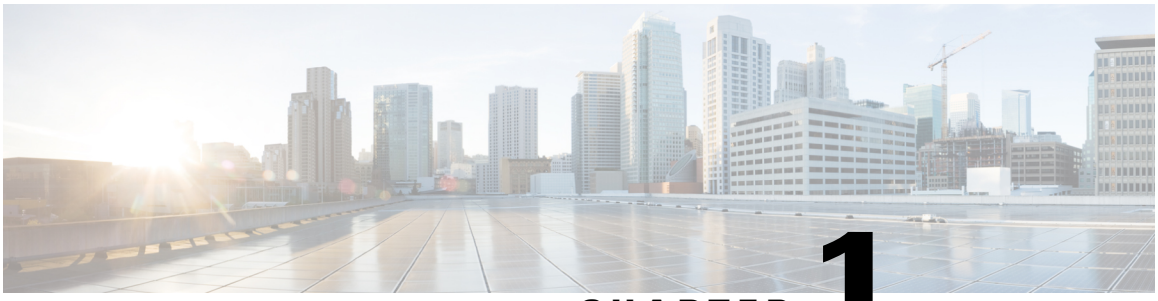
CHAPTER 7 **Documentation Updates 51**
License Mac References 52
Administration Guide 52
Access Control Group Permissions Interactions 52
Conference Bridge Section Updates 52
Disable Early Media on 180 Correction 53
Hostname and IP Address Field Can Contain a Fully Qualified Domain Name 53

Hostnames in IPv4 and IPv6 Environments 53
Hub_None Location Correction 53
An ILS Restart is Required for Changes to Directory URI Catalogs 53
Incorrect Information about Deleting Route Patterns 54
Incorrect Note about User Locales 54
Line Group Deletion Correction 55
Maximum Hunt Timer Restriction 55
Phone Support for Multilevel Precedence and Preemption 55
Transmit UTF8 for Calling Party Name Field Correction 55
Directory Number Field Description Updated 56
A Server Restart is Required After Uploading a Certificate 56
ILS Restictions for Directory URIs 56
Cisco Unified IP Phone setup Description Character Length 56
Correction in Software Conference Bridge Maximum Audio Streams 57
Call Detail Records Administration Guide 57
FAC and CMC Code is not Captured in CDR 57
CLI Reference Guide 60
ILS Troubleshooting Tips Corrections 60
Show perf query counter Command Output 60
Disaster Recovery System Guide 60
Cygwin SFTP Servers 60
Supported SFTP Servers 60
System Backup File Encryption 61
Updated Caution to Include DNS and Domain Name Prior To Restore 61
Features and Services Guide 62
Bulk Certificate Import May Cause Phones To Restart 62
Call Queuing Interaction with Hunt Groups and Hunt Pilots 62
Calling Party Normalization Restriction 62
Centralized Proxy TFTP File Signature Verification Failure 62
Cisco Unified Communications Manager Sends INVITE Message to VCS 63
Client Matter Codes, Forced Authorization Codes, and Failover Calls 63
Configuring OpenAM Section 63
Corrected License Report Update Interval 64
Corrections for the Immediate Divert Feature 64
EMCC Logout Limitation 65

Empty Far-End When Recording Call Park for Some Phones 66
Incorrect Report for Device Mobility 66
Jabber Devices Count as Registered Devices 66
Music On Hold and Native Call Queuing Behavior 66
New Audio Files for Music On Hold 66
Native Call Queuing Periodic Announcement Behavior 67
Remote Destination and Auto Answer 67
Video Capabilities and Enhanced Location Call Admission Control 67
Call Pickup Restriction 67
4000 Series Integrated Services Routers do not support Mobile Voice Access 68
Installing Cisco Unified Communications Manager 68
Installation Fails with Unrecoverable Internal Error 68
Presence Data Loss After Upgrade From Cisco Business Edition 5000 to Cisco Unified Communications Manager 69
Presence User Experiences Issues Obtaining Availability 69
Interdomain Federation for IM and Presence Service 70
Cannot Install Signed Microsoft CA Server-Client Authentication Certificate on Microsoft OCS 2008 70
FIPS Not a Requirement for Federated Connections with LYNC 2010 Servers 70
Use TLS for Static Routes 70
Partitioned Intradomain Federation for IM and Presence Service 71
Disable Empty TLS Fragments 71
FIPS Not a Requirement for Federated Connections with LYNC 2010 Servers 71
MatchUri Set to IM and Presence Service Domain 71
Use TLS for Static Routes 71
Managed Services Guide 71
SNMP Limits 71
Unified Communications Manager Alarms 72
Real-Time Monitoring Tool Guide 72
Analyze Call Path Tool does not Work with Non-English Language 72
Incorrect Default Value for LogPartitionLowWaterMarkExceeded Alert 72
LowAvailableVirtualMemory Threshold Value is Incorrect 73
CallProcessingNodeCpuPegging Alerts for VMware Installations 73
An RTMT Update Is Required When You Upgrade Unified CM 73
Upgrade RTMT 73

Security Guide 74
Bulk Certificate Import May Cause Phones To Restart 74
Incorrect Configuration Example for ASA Router 74
IP Phone SSL VPN not Supported on Third Party Firewalls 76
Replace ASA Certificate on AnyConnect VPN Phone 77
Secure and Nonsecure Indication Tone 77
CNF File Encryption Is Not Supported by Default on 6901 and 6911, Cisco IP Phones 78
ITL File Size Limitation 78
Serviceability Guide 78
AXL Web Service Requirement for ICSA HA 78
Cisco CAR DB Service 78
CAR Database Update 79
Cisco Certificate Change Notification Service 79
Cisco SOAP-CallRecord Service 79
Platform Administrative Web Service 79
SNMP Limits 80
IM and Presence Security Best Practice 80
SOAP-Diagnostic Portal Database Service 80
Error in SYSLOG-MIB Parameters 81
System Guide 81
Call Transfer to Hunt Pilot Restriction 81
Insufficient Information About Third-Party Restrictions 81
Video Resolution Support for SIP Phones 81
Time of Day routing not Implemented for Message Waiting Indicator 82
TCP and UDP Port Usage Guide 82
Corrected Port Information 82
Missing Information about TCP Port 22 83
Missing Information about TCP Port 5555 83
Missing Information about Common Service Port 8006 83
Upgrade Guide 84
Adding a New Subscriber Causes Device Reset 84
Special Characters in LDAP Password Cause Upgrade Failure 84
User Options Guide 84
The Fast Dial User Option is Not Supported 84
XML Developers Guide 84

Serviceability XML API Doc in Error 84
Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service 85
Domain Name Change for Cisco Unified Communications Manager 85
Update Domain Name for Cisco Unified Communications Manager 85
Online Help for Cisco Unified Communications Manager 86
Incorrect Description for Destination Number 86
Directory Number Field Description Updated 86
Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager 86
Retrieve Chat Rooms on a Replaced Node 86



CHAPTER 1

Introduction

- About Release Notes, page 1
- Hardware Server Requirements, page 2
- Server software requirements, page 4
- Supported browsers, page 4

About Release Notes

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

Unified Communications Manager, the call-processing component of the Cisco Unified Communications System, extends enterprise telephony features and capabilities to IP phones, media processing devices, VoIP gateways, mobile devices, and multimedia applications.

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

Note In the past, export licenses, government regulations, and import restrictions have limited the ability of Cisco to supply Unified Communications Manager and IM and Presence Service worldwide. Cisco has obtained an unrestricted U.S. export classification to address this issue.

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

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 1: Supported Servers for UPS Integration

HP servers	IBM servers
MCS-7816-H3	MCS-7816-I3
MCS-7825-H3	MCS-7816-I4

HP servers	IBM servers
MCS-7825-H4	MCS-7816-I5
MCS-7828-H3	MCS-7825-I3
MCS-7835-H2	MCS-7825-I4
MCS-7845-H2	MCS-7825-I5
	MCS-7828-I3
	MCS-7828-I4
	MCS-7828-I5
	MCS-7835-I2
	MCS-7845-I2
	MCS-7845-I3
	MCS-7845-I3

Server software requirements

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

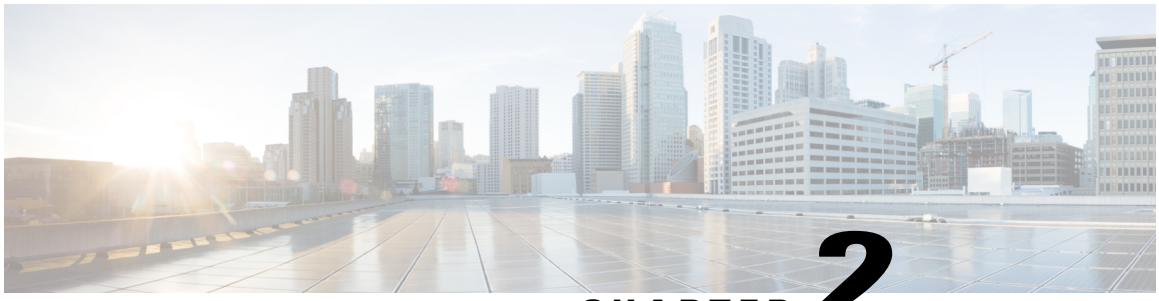
Supported browsers

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

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

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

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



CHAPTER 2

Unified Communications Manager Upgrade to Release 9.1(2)

- Software Version Number, page 5
- Pre-Upgrade Tasks, page 5
- Overview of Software Upgrade Process, page 8
- Upgrade on Virtual Server, page 8
- Configuration Changes During Upgrade, page 9
- Supported Upgrades, page 10
- Upgrade File, page 10
- Upgrade Media, page 10
- Software Upgrade Procedures, page 11
- Post-Upgrade Tasks, page 15
- Latest Software and Firmware Upgrades, page 15
- Related Documentation, page 16
- Limitations and Restrictions, page 16

Software Version Number

These release notes are based on the following software version of Unified Communications Manager:

9.1.2.10000-28

Pre-Upgrade Tasks

For customers who are upgrading from pre-9.0 releases (Releases 5.0 to 8.6) to any 9.x release, you must register all unused Product Authorization Keys (PAKs) and install all pre-9.0 licenses before you upgrade to

9.x. After you upgrade to the latest 9.x release, you will not be able to install pre-9.0 licenses onto a 9.x Enterprise License Manager.

For customers who are upgrading from pre-9.0 releases to 9.x, a license migration is required.

Before you upgrade to Cisco Unified Communications Manager Release 9.1(2), download and run the License Count Utility to gather data and submit a request to Cisco for a preupgrade license review report. This report is used for license migration to 9.x licenses.

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:

- "License Migration" topic in the New and Changed Information chapter.
- *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. (The upgrade is a Refresh Upgrade when the major OS version changes between the "from" version and "to" version. For Unified Communications Manager upgrades to 9.1(2), the upgrade executes a Refresh Upgrade when the "from" version is earlier than Release 8.6(x)).

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.

Also, see the new upgrade process available under the "Jump Upgrade" procedure.

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.

Upgrade on 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 were made to the OVAs:

- The number and the size of the vDisk for the 7500 user and 10,000 user OVAs changed from 2 x 80 GB to 1 x 110 GB. If your current virtual machine 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 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. For Unified Communications Manager upgrades to 9.1(2), the upgrade executes a Refresh Upgrade when the "from" version is prior to Release 8.6(x).

Procedure

Step 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.

Step 2 After you finish the upgrade, shut down the virtual machine.

Step 3 Change the Guest Operating System to Red Hat Enterprise Linux 5 (32-bit).

Step 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 the OVA file for this release 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.

Step 5 Save changes.

Step 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_v1.2.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 11.

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 11.

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 11.
2. If you are performing a Refresh Upgrade on HP7825H3 or HP7828H3 hardware from a version prior to Release 8.6(x), use an externally powered USB disk drive with a minimum size of 16 GB to migrate the data from the old system to the new installation. For Cisco Unity Connection and Cisco Business Edition 5000, an externally powered USB disk drive with a minimum size of 128 GB is required. Cisco recommends that you use an externally powered USB drive because other drives may not be recognized during the Refresh Upgrade sequence.

3 Put the upgrade file on an FTP or SFTP server that the server that you are upgrading can access.
4 Log in to Cisco Unified Communications Operating System Administration.
5 Navigate to **Software Upgrades** > **Install/Upgrade**.

   The Software Installation/Upgrade window displays.
6 From the Source list, choose **Remote File system**.
7 In the **Directory** field, enter the path to the directory that contains the patch file on the remote system.

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

   If the upgrade file is located on a Windows server, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax. Begin the path with a forward slash and use forward slashes throughout the path. The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).
8 In the **Server** field, enter the server name or IP address.
9 In the **User Name** field, enter the user name on the remote server.
10 In the **User Password** field, enter the password on the remote server.
11 Select the transfer protocol from the **Transfer Protocol** field.
12 To use the Email Notification feature, enter your Email Destination and SMTP Server in the fields provided.
13 To continue the upgrade process, click **Next**.
14 Choose the upgrade version that you want to install and click **Next**.
15 In the next window, monitor the progress of the download.

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

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

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

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

16 If you want to install the upgrade and automatically reboot to the upgraded software, choose **Switch to new version after upgrade**. The system restarts and runs the upgraded software.
17 If you want to install the upgrade and then manually switch to the upgraded software at a later time, choose **Do not switch to new version after upgrade**.
18 Click **Next**. For a Refresh Upgrade, the following text appears:

   - For non- HP7825H3/HP7828H3 hardware:

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

   - For HP7825H3/HP7828H3 hardware:

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

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

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

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

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

Bridge Upgrade

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

Post-Upgrade Tasks

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

- Install additional locales
- Install COP files

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

Latest Software and Firmware Upgrades

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

Firmware

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

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

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

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

Software

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

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

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

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

Related Documentation

You can view documentation that is associated with supported applications.

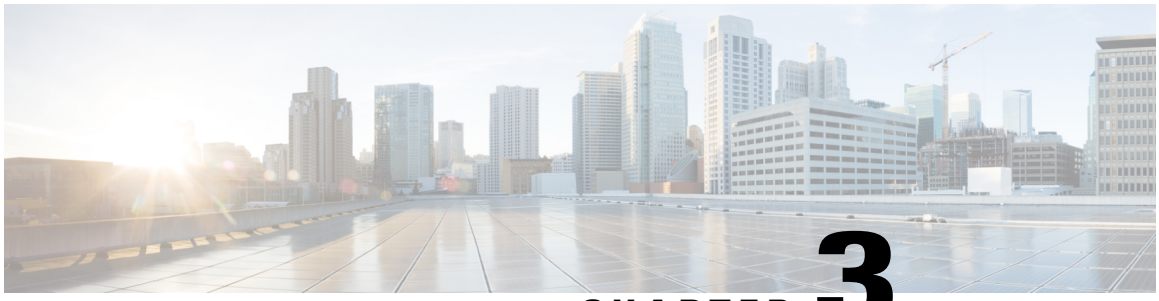
Application	Documentation Link
Cisco Unified Communications Manager	http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html
Cisco Unified Contact Center Express	http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/tsd-products-support-series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

Limitations and Restrictions

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

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

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



CHAPTER 3

IM and Presence Service Upgrade to Release 9.1(1a)

- New system installation information, page 19
- System Upgrade, page 19
- Upgrade order, page 21
- Software licensing requirements for VMware, page 21
- Recommendations for Release 8.0(x), 8.5(x), or 8.6(x) to 9.1(1) Upgrades, page 21
- OS Administrator Account Required for IM and Presence Upgrades, page 22

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

IM and Presence Service Release 9.1(1a) is compatible with Unified Communications Manager Release 9.1(2).

Supported Upgrade Paths to IM and Presence Service Release 9.1(1a)

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

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(1a)	Upgrades from Release 8.0(1) through 8.6(1) to Release 9.1(1a) 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 9.0(1) to Release 9.1(1a) 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(1a) 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: 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.

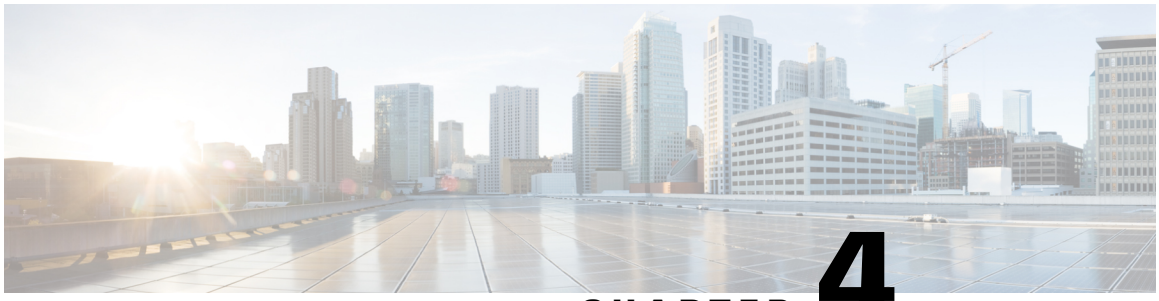
- **Contact List Size**

  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.

OS Administrator Account Required for IM and Presence Upgrades

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

Please note that this limitation exists for IM and Presence Service only and does not apply to Cisco Unified Communications Manager. Also note that this limitation may be fixed for newer ISO files. Refer to your ISO Readme file for ISO-specific details. See CSCvb14399 for updated defect details.



CHAPTER 4

Important Notes

- 60 GB 9.x UCM VM Deployed From OVA Has Unaligned Partitions, page 23
- Bridge Upgrade Fails with Insufficient Disk Space, page 24
- Call Forward Notification All Lines, page 24
- Cannot Add Subscriber When Performing Cisco Business Edition 5000 to Cisco Business Edition 6000 Migration, page 25
- Changed License Calculations for Extension Mobility, page 25
- Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets, page 25
- Cisco Unified Mobility Disclaimer, page 26
- Configure LDAP Directory, page 26
- Jabber Certificate Warnings with IM and Presence Service, page 26
- Migrating Phones Between Clusters, page 27
- Partition Alignment Check in VMware Installation CLI and GUI, page 27
- Phone Support for URI Dialing Display Preference Service Parameter, page 28
- Upgrade to 9.1(1) Fails with Insufficient Disk Space, page 28
- Devices Reset while Certificate Regeneration, page 29
- MGCP IOS Gateway From PSTN Does Not Support Connected Address in ISDN Notify , page 29
- Perfect Forward Secrecy is not Supported in IPsec Configuration, page 29
- Change Perfmon Counter File Size Parameters in RTMT, page 30

60 GB 9.x UCM VM Deployed From OVA Has Unaligned Partitions

This information applies to CSCuh07443.

Unified Communications Manager 9.x virtual machines that were created with a v1.6 or older OVA, such as cucm_9.1_vm7_v1.6.ova, and deployed with the “CUCM 2500 user node - 60GB hard drive” configuration have unaligned partitions. These VMs could have been installed with Unified Communications Manager

9.0(1). However, Unified Communications Manager 9.1(2) adds a feature to the VMware Installation information line to indicate whether the disk partitions are aligned. Therefore, this issue of these partitions being unaligned is apparent after upgrading to Version 9.1(2).

If your virtual machine is in this state, Cisco cannot provide support for performance issues. To correct the unaligned disk partitions, you must perform the following actions:

1. Take a DRS backup of the system.
2. Deploy a new virtual machine from an updated version of the OVA (v1.7 or later) and perform a fresh installation of the previously unaligned virtual machine. Details can be found on this Virtualization DocWiki page: http://docwiki.cisco.com/wiki/Implementing_Virtualization_Deployments.
3. Perform a restore operation on the freshly installed node, using the DRS backup taken in Step 1.

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(2), perform one or more of the following actions to create more disk space on the partition:

- Follow the jump upgrade process instead of doing a bridge upgrade on a physical server.
- Upgrade the hard drives on the bridge upgrade server to 80GB or higher, and perform the bridge upgrade again.

Call Forward Notification All Lines

This information applies to CSCui20684.

This parameter determines whether the Forward All notification is sent only to the primary line or to all the configured lines of the phone. If set to FALSE (default), then Forward All notification is sent only to primary line of the phone. If set to TRUE, Forward All notification is sent to all the configured lines of the phone.

For new phone models, when a nonprimary line is set to Call Forward All, the phone icon that corresponds to that line can show Diversion indication. With the service parameter, if you are using the shared line with phone models such as 7940 or 7960, Unified Communications Manager will not send Forward All Notification to nonprimary lines. If you have phone models such as 8961, 6961, and TNP phones with a supported phone load, then you can enable the service parameter so that Forward All Notification is sent to all lines.

For new phone models, when a nonprimary line is set to Call Forward All, the phone icon that corresponds to that line can show Diversion indication. However, phone models such as 7940 or 7960 do not support Forward All notification on any lines. If you are using the shared line with phone models such as 7940 or 7960, set the service parameter to Disable so that Unified Communications Manager will not send Forward All Notification to nonprimary lines. If you have phone models such as 69XX, 89XX, or 797X or do not use

multiple shared lines, then you can enable the service parameter so that Forward All Notification is sent to all lines.

When you upgrade from Unified Communications Manager between Releases 8.6(2.24081.x) and 8.6(2.24089.x) or 9.1(1) to 9.1(2), the behavior changes and by default you will not see Forward All notification on nonprimary lines for SCCP phones. If you need to see the Forward notification on nonprimary lines and have only new phone models, then you must enable this service parameter to get the Forward All notification on nonprimary lines on SCCP phones.

When you upgrade from Unified Communications Manager pre-8.6(2.24081.001) or between post-8.6(2.24089.x) and pre-9.1(1) to 9.1(2), the behavior does not change.

Cannot Add Subscriber When Performing Cisco Business Edition 5000 to Cisco Business Edition 6000 Migration

This information applies to CSCuj84092.

When you export Bulk Administration Tool data from Cisco Business Edition 5000, uncheck the Enterprise Parameter check box. If this check box remains checked, you cannot add a new subscriber to Cisco Business Edition 6000.

Changed License Calculations for Extension Mobility

This information applies to CSCue14471.

The Cisco Extension Mobility feature consumes an essential license for Unified Communications Manager 9.0(1) through 9.1(1). With 9.1(1a) this is changed; a user configured with Extension Mobility (device profiles configured under Extension Mobility) only will no longer consume an Essential license. So, a user configured with Extension Mobility only, with no other devices assigned, will not consume an Essential license.

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

This information applies to CSCtn79567.

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

Cisco Unified Mobility Disclaimer

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

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

Configure LDAP Directory

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

Note This is an updated list for this release.

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

Jabber Certificate Warnings with IM and Presence Service

This information applies to CSCum63324.

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

Migrating Phones Between Clusters

This information applies to CSCup87451.

When you perform a jump upgrade to Release 9.1(2) and migrate phones between clusters, you must take steps before you begin the migration to ensure that the phones can update their Initial Trust List (ITL) files.

When an ITL file is installed on a phone, all future configuration files and ITL file updates must be either:

- Signed by the CCM+TFTP Server certificate currently installed in the phone's CTL file (if cluster security with CTLs is enabled).
- Signed by the CCM+TFTP Server certificate installed in the phone's ITL file.
- Signed by a certificate that exists in one of the Cisco Unified Communication Manager server TVS certificate stores that are listed in the ITL file.

If phones are unable to update their ITL files, you cannot make changes to the phones through TFTP or HTTP configuration files. To avoid this issue, include one of the following options in your migration plan:

- Bulk Certificate Export—Use this option if both clusters are online with network connectivity while the phones are being migrated.
- Rollback Enterprise Parameter—This option is valid only if you complete it before you attempt the phone migration.
- Hardware Security Tokens—Use this option if hardware security tokens have been used to generate a CTL (Certificate Trust List) on both the old and new clusters.

For detailed information about each of these options, see *Migrating Phones Between Clusters with Cisco Unified Communications Manager 8 and ITL Files* at https://supportforums.cisco.com/document/60716/migrating-ip-phones-between-clusters-cucm-8-and-itl-files.

Partition Alignment Check in VMware Installation CLI and GUI

This information applies to CSCug69836.

Unified Communications Manager 9.1(2) adds a feature to the VMware Installation information line to indicate whether the disk partitions are aligned. When you install Unified Communications Manager in a virtual machine that is created or deployed from the Cisco-generated OVA template, the disk partitions are aligned and the VMware installation information line will indicate “Partitions aligned.”

If your installation of Unified Communications Manager was not properly performed using the Cisco-generated OVA template to create the virtual machine, the disk partitions are unaligned. The VMware installation information line will indicate “ERROR-UNSUPPORTED: Partitions unaligned.” If your virtual machine is in this state, Cisco cannot provide support for performance issues. To correct a virtual machine with unaligned partitions you must perform the following actions:

1. Take a DRS backup of the system.
2. Deploy a new virtual machine from the Cisco-generated OVA template and perform a fresh installation of the previously unaligned virtual machine. For details, see the Virtualization DocWiki page: http://docwiki.cisco.com/wiki/Implementing_Virtualization_Deployments.
3. Perform a restore operation on the freshly installed node, using the DRS backup taken in Step 1.

After you perform these steps, your virtual machine will have aligned partitions.

Note You must follow this same alignment correction process as part of the newly added Jump Upgrade procedure that allows an existing Unified Communications Manager 6.1/7.1 environment to be installed and restored on VMware for the purpose of upgrading directly to Version 9.1(2). Because Unified Communications Manager versions prior to 8.0(2) are not supported on VMware, installations of these versions even when using the Cisco-generated OVA template have unaligned disk partitions.

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.”

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.

Devices Reset while Certificate Regeneration

This update is applicable for CSCus63274.

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

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

This information applies to CSCut08346.

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

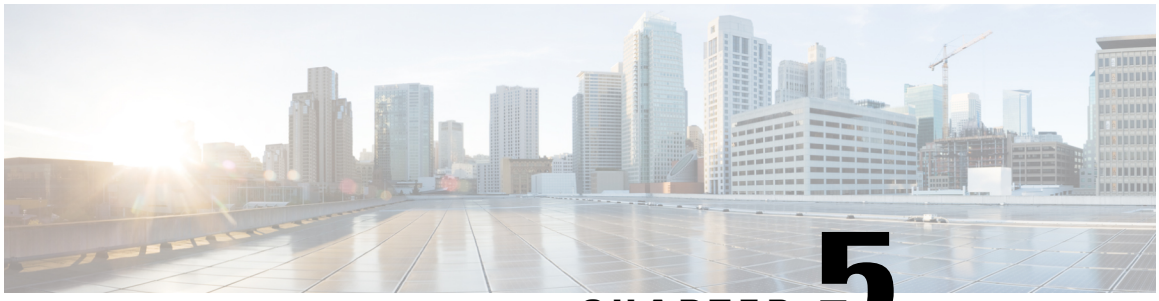
Perfect Forward Secrecy is not Supported in IPsec Configuration

This information applies to CSCuu74346.

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

Change Perfmon Counter File Size Parameters in RTMT

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



CHAPTER 5

New and Changed Information

- Jump Upgrade, page 31
- License Migration, page 32
- New CLI Commands for Release 9.1(2), page 36
- iX Media Channel, page 37
- Include Partition Alignment Check in VMware Installation CLI and GUI, page 37
- V.110 (Clear Channel Codec) Enhancement to Support GSM Networks, page 38
- Cisco Voice Gateways (ISR) 44XX Series , page 38

Jump Upgrade

Jump Upgrade is a simplified upgrade process that allows migration from Unified Communications Manager Release 6.1(4), 6.1(5), 7.1(3) and 7.1(5) on an MCS platform to a Virtualized platform, in a controlled lab environment, followed by switchover to the production network.

Jump Upgrade replaces the need for interim hardware as required by Bridge Upgrade, when existing hardware does not support Unified Communications Manager Release 9.1(2). It enables the migration by performing the upgrade in an isolated network, without affecting your existing production network.

The jump upgrade is performed in four stages:

1. Upgrade to Unified Communications Manager Release that supports jump upgrade. Choose one of Unified Communications Manager 6.1(4)/(5) or 7.1(3)/(5) as an intermediate release, on your existing hardware.
2. Virtualize your current release in an isolated environment.
3. Upgrade the virtualized cluster to Unified Communications Manager Release 9.1(2).
4. Rebuild Unified Communications Manager virtual machines to align disk partitions.

The jump upgrade procedure applies to Unified Communications Manager clusters with the following environment:

- One of the following Unified Communications Manager releases is installed: Releases 4.1(3) to 4.3(2), Releases 5.1(2) to 5.1(3), or Releases 6.0(1) to 7.1(5).

- None of the current hardware supports Unified Communications Manager Release 9.1(2) or migration to a virtual platform is desired.
- The upgrade to Release 9.1(2) and data migration will be performed in an isolated environment and moved to production during a service window.

For more information, see *Jump Upgrade Procedure for Cisco Unified Communications Manager Release 4.1(3)–7.1(5) to 9.1(x)* on Upgrade Central: https://communities.cisco.com/community/partner/collaboration/migration.

Note The installation of COP file will abort giving an error message if NTP (Network time protocol) is not configured on the VMWare platform, for releases earlier than 7.1.5

License Migration

For the Cisco Unified Communications Manager Release 9.1(2), the license migration process has been revised for a supported manual license migration:

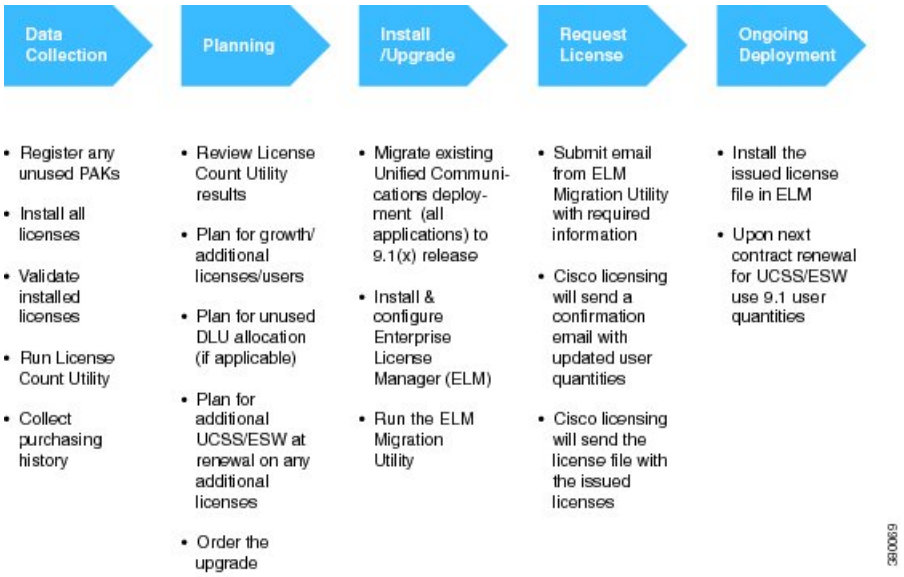
- License Count Utility has been revised to support data gathering and submittal of the request for a preupgrade license review report. It is a pre-requisite to run the License Count Utility prior to upgrading Cisco Unified Communications Manager to version 9.1.
- Enterprise License Manager migration utility for license migrations for Cisco Unified Communications Manager User Connect License (UCL) and Cisco Unified Workspace License (UWL) customers has been revised to support data gathering and submittal of the request for license migration to Cisco licensing (licensing@cisco.com).
- Enterprise License Manager migration utility for license migrations for Cisco Unity Connection Cisco Unified Workspace Licenses (UWL) customers has been revised to support data gathering and submission to Cisco licensing (licensing@cisco.com).

Cisco Unified Communications Manager Release 9.1(2) supports manual license migration. Before you upgrade to Cisco Unified Communications Manager Release 9.1(2), download and run the License Count Utility to gather data and submit a request to Cisco for a preupgrade license review report. User Connect License (UCL) and Cisco Unified Workspace License (UWL) customers can use the Enterprise License Manager Migration Utility to gather data and submit requests for license migration to Cisco licensing at licensing@cisco.com.

Cisco Unified Communications Manager Migration Process Overview

For customers who are upgrading from pre-9.0 releases to 9.x, a license migration is required.

The process overview for Cisco Unified Communications Manager license migration is as follows:



See the following procedures for a more detailed description of each step.

Data Collection Before Upgrade

Follow this procedure to collect licensing data before you upgrade.

Procedure

Step 1 Register any unused PAKs using the Product License Registration site: www.cisco.com/go/license.

- You cannot fulfill a pre-Release 9.x license PAK to an Enterprise License Manager.

Step 2 Install all licenses.

- This ensures that all license counts are considered for the migration.
- You must install all pre-Release 9.x licenses to Unified Communications Manager before you upgrade. Following the upgrade, you cannot install pre-Release 9.x license to the Enterprise License Manager.

Step 3 Validate installed licenses.

a) Go to **Cisco Unified Communications Manager Administration > System > License Unit Report**. Status will be “Uploaded” for the Phone License Feature, CCM Node License Feature, and Software License Version.

If status is not “Uploaded,” then your migration may not bring over this legacy license information.

b) Use Snapshot license usage to verify device counts. From the Cisco Unified Communications Manager Administration page, select **System > License Unit Report** and **License Unit Calculator** windows.

Step 4 Run License Count Utility (LCU).

- The License Count Utility, which often appears under the name User Count Tool, is used for planning migrations for Cisco Unified Communications Manager to Cisco Unity Connection Release 9.x licensing. It supports migrations from Unified Communications Manager Releases 6.x to 8.x migration to Cisco Unity Connection Release 9.x.
- License Count Utility is found on the Software Download Center under Unified Communications Manager Release 8.6 Utilities.
- Go to www.cisco.com/go/software, select **Products > Voice and Unified Communications > IP Telephony > Unified Communications Platform > Cisco Unified Communications Manager (CallManager) > Cisco Unified Communications Manager Version 8.6 > Unified Communications Manager > CallManager > Cisco Unity Connection Utilities-LCU**.
- Use UCT release 2.1 if upgrading to 9.1(1).
- Use LCU release 9.1.2 if upgrading to 9.1(1a) or 9.1(2).
- Submit the License Count Utility output to licensing@cisco.com and request a Pre-Upgrade License Review to receive license migration counts for premigration planning.
- If you are using LCU Release 2.1, also include the **From** and **To** Unified Communications Manager release; the **From License MAC**, and UCSS/ESW contract numbers.
- If you are using a pre-6.x release of Unified Communications Manager, submit a device inventory (quantity per device type), planned user counts and, if users will use Mobility, user counts for multiple devices and the license usage screenshot (if Release 5.x).

Step 5 Collect purchasing history.

- Were the licenses purchased as UCL or UWL or both?
- What were the purchased quantities and type of users?
- Do you have service contracts?

If additional information on UCSS Contracts is needed, contact the UCSS Support team ucss-support@external.cisco.com.

Planning Before Upgrade

Follow this procedure to plan your licensing requirements before you upgrade.

Procedure

Step 1 Review License Count Utility (LCU) results.

- Use the Pre-Upgrade License Review Report received from licensing@cisco.com to review and compare the recommended or required license counts to your purchasing history.

- If you have questions about the data or the process, contact licensing@cisco.com and reference your previous service request.

Step 2 Plan for growth.

- Take your typical growth into account for additional licenses required.
- For UCL customers, plan for unused DLU allocation.
- Plan for updates to service contracts if additional licenses are required.

Step 3 Order the upgrade (and service contracts if applicable).

- If ordering under a service contract, place the order from the Product Upgrade Tool, http://tools.cisco.com/gct/Upgrade/jsp/index.jsp, and plan for user migration.
- If not under a service contract, order from your partner or from the ordering tools directly. Order the migration based on the number of licenses required plus your planned growth.

Installation and Upgrade

Procedure

Step 1 Migrate existing Unified Communications deployments to Release 9.1:

- Upgrade products to Unified Communications Release 9.1.
- Products will run for a 60-day demo period initially with no connection to Enterprise License Manager or no licenses installed.

Step 2 Install and configure Enterprise License Manager:

- Use Enterprise License Manager installed Coresident with the product installations or install Enterprise License Manager as a standalone.
- Connect Enterprise License Manager to the product instances by adding the products to the Enterprise License Manager product inventory.
- Synchronize and verify a successful connection to Enterprise License Manager.

Step 3 Run the Enterprise License Manager Migration Utility:

a) From Enterprise License Manager, select **License Management > License Planning > Migrate Licenses to Enterprise License Manager**.
b) Select the Unified Communications Manager product type and include the Cisco Unified Communications Manager instances for license migration.
c) Enter the requested information. Click **Finish and Generate Request**.

Request Licenses

Follow this procedure to request licenses.

Procedure

Step 1 Send the email message from Enterprise License Manager Migration Utility:

- Attach the License Count Utility Pre-Upgrade Report
- Email is generated and, when sent, goes to licensing@cisco.com.
- A confirmation email with service request number for your licensing case is returned. Licensing will contact you if further information is required.

Step 2 Cisco Licensing sends a confirmation email with updated user quantities.

Step 3 Cisco Licensing sends the license file with the issued licenses.

Deployment

Procedure

Step 1 Install the issued license file in Enterprise License Manager.

- From Enterprise License Manager, select **License Management > Licenses > Fulfill Licenses from File**.

Step 2 Upon next contract renewal for UCSS/ESW, use Release 9.1 user quantities.

- 90 days prior to contract expiration, contact sales to arrange for contract renewal.
- Base user counts on Release 9.1 user quantities plus any incremental growth.
- Enterprise License Manager usage reports may be used to determine user counts at the time of renewal.

New CLI Commands for Release 9.1(2)

The following CLI commands have been added for Enterprise License Manager Release 9.1(2):

- **license management reset identity**

This command resets the licensing identity of the Enterprise License Manager server and removes all installed licenses. You must perform a license rehost to recover any license that was previously installed on this server. This operation may take a few minutes to complete.

- **license management product reregister all**

  This command removes any registration conflict by reregistering all the product instances to this Enterprise License Manager server. This command may take some time for re-registration and synchronization with all product instances to complete.

- **license file diagnose** {**full**}

  This command enables you to select a license file from a list and print diagnostic information.

- **license file get** {**compress**}

  This command creates a TAR file of the license file or files on the system and transfers the TAR file to a remote area.

iX Media Channel

The iX Media Channel feature provides a simple, reliable, and secure channel for multiplexing multiple application layer protocols. To enable support for iX Media Channel on a SIP trunk, choose **Device** > **Device Settings** > **SIP Profile** in Cisco Unified Communications Manager Administration and check the **Allow iX Application Media** check box.

Note Unified Communications Manager supports iX Media Channel negotiation only when a video channel has been established.

Note For supported SIP devices, iX Media Channel must be enabled from the device user interface. For more information, see documentation related to your phone model.

Include Partition Alignment Check in VMware Installation CLI and GUI

Unified Communications Manager 9.1(2) adds a feature to the VMware Installation information line to indicate whether the disk partitions are aligned. When you install Unified Communications Manager in a virtual machine created/deployed from the Cisco-generated OVA template, the disk partitions are aligned and the VMware installation information line will indicate "Partitions aligned".

If your installation of Unified Communications Manager was not properly performed using the Cisco-generated OVA template to create the virtual machine, the disk partitions are unaligned. The VMware installation information line will indicate "ERROR-UNSUPPORTED: Partitions unaligned". If your virtual machine is in this state, Cisco cannot provide support for performance issues. To correct a virtual machine with unaligned partitions you must perform the following actions:

1. Take a DRS backup of the system.
2. Deploy a new virtual machine from the Cisco-generated OVA template and perform a fresh install of the previously-unaligned virtual machine. Details can be found on this Virtualization DocWiki page: http://docwiki.cisco.com/wiki/Implementing_Virtualization_Deployments.
3. Perform a restore on the freshly-installed node, using the DRS backup taken in Step 1.

After performing these steps, your virtual machine will have aligned partitions.

Note You must follow this same alignment correction process as part of the newly-added Jump upgrade procedure that allows an existing Unified Communications Manager 6.1/7.1 environment to be installed and restored on VMware for the purpose of upgrading directly to version 9.1(2). Because Unified Communications Manager versions prior to 8.0(2) are not supported on VMware, installations of these versions even when using the Cisco-generated OVA template have unaligned disk partitions.

V.110 (Clear Channel Codec) Enhancement to Support GSM Networks

This release includes an enhancement to the V.110 (Clear Channel Codec) that supports calls going through the slower GSM network. The following are required to use this enhancement:

- Service parameter **Allow Layer 1 info for Pri Bearer Capability for V110 calls** is set to True
- MGCP gateway is in a PRI to PRI configuration using V.110 (Clear Channel Codec)
- G.Clear enabled on the gateway

Note The enhancement is limited to PRI to PRI calls within a Unified Communications Manager cluster. The enhancement does not work over SIP or H.323 intercluster trunks.

Cisco Voice Gateways (ISR) 44XX Series

The following list provides available interfaces that Cisco Unified Communications Manager supports with Integrated Services Route (ISR) 44XX series gateways:

- T1 CAS/PRI and E1/PRI signaling using MGCP
- T1/PRI and PRI using SIP or H.323

Cisco ISR44XX Series Gateways

The Cisco Integrated Services Router 44XX series gateways are Integrated Services Router family gateways with multi-core capability.

The key features of the gateways are:

- Runs on BinOS in different cores.
- Provides Services Integration for Wide area application services (WAAS), Application Firewall, Video, Application Visibility, and so on in different cores.
- Provides manageability to the next level.

Cisco Integrated Services Router 4451-X

The Cisco Integrated Services Router 4451-X is a modular router, with LAN and WAN connections, that is configured by means of interface modules, Cisco Enhanced Service Modules (SM-Xs), and Network Interface Modules (NIMs).

The router provides encryption acceleration, voice and video capable architecture, application firewall, call processing, and embedded services.

The Cisco ISR 4451-X supports different wired interfaces such as T1 CAS/PRI and E1/PRI signaling using MGCP, T1/PRI and PRI using SIP or H.323, and fiber Gigabit Ethernet.

Cisco Voice Gateways

Cisco Unified Communications Manager supports several types of Cisco Unified Communications gateways. Gateways use call-control protocols to communicate with the PSTN and other non-IP telecommunications devices, such as private branch exchanges (PBXs), key systems, analog phones, fax machines, and modems.

Trunk interfaces specify how the gateway communicates with the PSTN or other external devices by using time-division-multiplexing (TDM) signaling. Cisco Unified Communications Manager and Cisco gateways use a variety of TDM interfaces, but supported TDM interfaces vary by gateway model.

The following list provides available interfaces that Cisco Unified Communications Manager supports with MGCP gateways:

- Foreign Exchange Office (FXO)
- Foreign Exchange Station (FXS)
- T1 Channel Associated Signaling (CAS) recEive and transMit or ear and mouth (E&M)
- Basic Rate Interface (BRI) Q.931
- T1 PRI-North American ISDN Primary Rate Interface (PRI)
- E1 PRI-European ISDN Primary Rate Interface (PRI)

The following list provides available interfaces that Cisco Unified Communications Manager supports with H.323 gateways:

- FXO
- FXS
- E&M
- Analog Direct Inward Dialing (DID)

- Centralized Automatic Message Accounting (CAMA)
- BRI Q.931
- BRI QSIG-Q signaling protocol that is based on ISDN standards
- T1 CAS FXS, FXO, and E&M
- T1 FGD
- T1/E1 PRI
- T1 PRI NFAS
- T1/E1 QSIG
- J1

The following list provides available interfaces that Cisco Unified Communications Manager supports with SCCP gateways:

- FXS

Cisco Unified Communications Manager can use H.323 gateways that support E1 CAS, but you must configure the E1 CAS interface on the gateway.

The following list provides available interfaces that Cisco Unified Communications Manager supports with Integrated Services Route (ISR) 44XX series gateways:

- T1 CAS/PRI and E1/PRI signaling using MGCP
- T1/PRI and PRI using SIP or H.323
- Analog FXS, FXO and BRI using MGCP
- Analog FXS and BRI using SCCP
- Analog FXS, FXO and BRI using SIP or H.323

The following list provides available interfaces that Cisco Unified Communications Manager supports with Integrated Services Route (ISR) 43XX series gateways:

- T1 CAS/PRI and E1/PRI signaling using MGCP
- T1/PRI and E1/PRI using SIP or H.323
- Analog FXS, FXO and BRI using mgcp
- Analog FXS and BRI using sccp
- Analog FXS, FXO and BRI using SIP or H.323

Standalone Voice Gateways

This section describes these standalone, application-specific gateway models that are supported for use with Cisco Unified Communications Manager.

Cisco VG310 Analog Phone Gateway

The Cisco VG310 is a medium-density 24-FXS port standalone Analog Voice Gateway that allows analog phones, TDM PBXs, fax machines, modems, and speakerphones to register with Cisco Unified Communications Manager or similar enterprise voice systems.

This gateway supports OPX-Lite analog ports, T1 CAS/PRI, E1/PRI , T1/PRI, PRI and BRI interfaces using SIP, SCCP, MGCP, H.323, and T.38 fax protocols.

Cisco VG320 Analog Phone Gateway

The Cisco VG320 is a medium-density 48-FXS port standalone Analog Voice Gateway that allows analog phones, TDM PBXs, fax machines, modems, and speakerphones to register with Cisco Unified Communications Manager or similar enterprise voice systems.

This gateway supports OPX-Lite FXS analog ports, T1 CAS/PRI, E1/PRI, T1/PRI, PRI and BRI interfaces using SIP, SCCP, MGCP, H.323, and T.38 fax protocols.

Cisco VG350 Analog Phone Gateway

The Cisco VG350 is a high density 144 standard FXS port and 96 OPX-Lite FXS port standalone Analog Voice Gateway. It allows analog phones, fax machines, modems, and speakerphones to register with Cisco Unified Communications Manager or similar enterprise voice systems.

This gateway supports four EHWIC slots for additional FXS, FXO ports, SIP, SCCP, MGCP, H.323, and T.38 fax protocols.

Voice Gateway Model Summary

The following table summarizes Cisco voice gateways that Cisco Unified Communications Manager supports with information about the supported signaling protocols, trunk interfaces, and port types.

Table 2: Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Port Types

Gateway Model	Supported Signaling Protocols	Trunk Interfaces	Port Types	Notes
Cisco ISR 4451-X	MGCP	T1/CAS/PRI E1/PRI		
	H.323 and SIP	T1/CAS/PR PRI		
Cisco VG310	MGCP	T1/CAS/PRI E1/PRI	FXS/FXO	
	H.323 and SIP	T1/CAS/PRI PRI		

Gateway Model	Supported Signaling Protocols	Trunk Interfaces	Port Types	Notes
Cisco VG320	MGCP	T1/CAS/PRI E1/PRI	FXS/FXO	
	H.323 and SIP	T1/CAS/PRI PRI		
Cisco VG350	MGCP	T1/CAS/PRI E1/PRI	FXS/FXO	
	H.323 and SIP	T1/CAS/PRI PRI		

CHAPTER 6

Caveats

- Bug Search Tool, page 43
- Resolved Caveats, page 44
- Open Caveats, page 44

Bug Search Tool

The system grades known problems (bugs) according to severity level. These release notes contain descriptions of the following bug levels:

- All severity level 1 or 2 bugs
- Significant severity level 3 bugs
- All customer-found bugs

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

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

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

Follow these steps to use Cisco Bug Search tool:

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

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

Resolved Caveats

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

Tip

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

Related Topics

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

Open Caveats

The following sections describe possible unexpected behaviors in Unified Communications Manager Release 9.1(2) and IM and Presence Service Release 9.1(1a).

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

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

When you open the online record for a defect, you see data in the "Fixed-In" field. The information that displays in this field identifies the list of interim versions in which the defect was fixed. These interim versions are then integrated into Unified Communications Manager or IM and Presence releases.

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

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

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

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

Related Topics

Bug Search tool

Open Caveats for Unified Communications Manager Release 9.1(2)

The following table lists open caveats that may cause unexpected behavior in Unified Communications Manager Release 9.1(2). These caveats may also be open in previous releases. The caveats are listed in alphabetical order by component and then in numerical order by severity.

Table 3: Open Caveats for Unified Communications Manager Release 9.1(2)

Identifier	Severity	Component	Headline
CSCue66813	3	alarm-library	Denial of Service on CUCM via GetDeviceProfile
CSCua71798	3	axl	Unable to update HuntPilot that does not have call queuing enabled
CSCud10175	3	backup-restore	DRS screen does not work on Chrome Mac
CSCue81560	3	bat	Insert RDP using BAT tool should not stop on one failed row
CSCug56813	3	bps-bat	Using BAT to change shared DN of one or more phone changes it on all
CSCud67438	3	ccm-serviceability	Unified Serviceability Tools can not connect to other nodes
CSCty02858	3	cmcti	Get platform exception on transfer with multiple hold and resume

Identifier	Severity	Component	Headline
CSCuc97126	3	cmcti	CTIRD to release the shared line initiated call in LmKeySetupReq
CSCug14142	3	cmui	Custom Access Control Group and Role not working for CCM User page
CSCuc87927	3	cmui	EUPLA URI Format
CSCud21579	3	cmui	UOP - Multiple issues with ring settings parameters
CSCud25151	3	cp-cac	Need better way to generate the random TID
CSCue48000	3	cp-callqueuing	Queue status on phoneTUI , incorrect "longest idle time" is displayed
CSCud05776	3	cp-device-manager	remote device remain unregistered after changing device pool
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
CSCud29378	3	cp-mediacontrol	CUCM does not proxy 200OK from Conductor to VCS
CSCuc96951	3	cp-mediacontrol	Encrypted call over SIP trunk to H323 gw drops
CSCuc94309	3	cp-mediacontrol	Extra resources allocated on MTP even with passthru disabled on DO call
CSCuc94411	3	cp-mediacontrol	Incorrect comparison for process name
CSCug13730	3	cp-mobility	Call Leak When Dual-Mode Connection Is Lost During User Control VMA Call
CSCue81468	3	cp-mobility	SNR to URI based Remote destination cannot be turned off from user pages
CSCuc73972	3	cp-sip-station	No Video when Blind Conference call is setup through TNP
CSCuo71657	3	cp-sip-station	Transcoder not inserted when SIP phone codec locked for recording
CSCuf81116	4	cp-sip-trunk	SIPInterface should not negotiate video when there is no video BW config
CSCuc89953	3	cp-supplementary-services	SIP MCU Conference unregisters from CUCM after two resets

Identifier	Severity	Component	Headline
CSCuf76965	3	cpi-appinstall	After COP installation there is a message to specify Reboot not Required
CSCuf46934	3	cpi-appinstall	DNS input bug
CSCud68399	3	cpi-appinstall	MCS7825H3- Upgrade failure in post-install phase boots to newer version
CSCue82671	3	cpi-os	DBUS-GLIB Message Sender Privilege Escalation (CVE-2013-0292)
CSCue55450	3	cpi-os	Remote Support Account Password Creation is Insecure
CSCtn39668	3	cpi-os	RHEL4AS Kernel Vulnerabilities
CSCua84906	3	cpi-os	SSL/TLS Protocol Information Disclosure (CVE-2011-3389)
CSCug37208	3	cpi-os	Tomcat core files are not generated in 9.0
CSCuc72621	3	cpi-os	Update JDK to 6.0-38 to Address Numerous Published Vulnerabilities
CSCug68766	3	cpi-platform-api	tomcat using more than 100 sessions
CSCue48971	3	cpi-third-party	OpenSSL OCSP Invalid Key Denial of Service Vulnerability (CVE-2013-0166)
CSCue48950	3	cpi-third-party	OpenSSL SSL/TLS and DTLS Plaintext Recovery Attack Vul (CVE-2013-0169)
CSCud52162	3	cuc-tomcat	Tomcat FORM Auth and CRSF Guard Vuls (CVE-2012-3546,CVE-2012-4431)
CSCuf17710	3	cuc-tomcat	Potential Clickjacking via Frameable Responses
CSCuc78854	4	cuc-tomcat	HTTP and HTTPS Ports DoS During TCP Connection Flood
CSCuc22587	3	database	CUCM DB Replication takes a long time to repair componentversion table
CSCue23203	3	dial-num-analyser	HTTP Status 500 java.lang.NullPointerException with DNA
CSCud21371	4	elm	JPN: ELM: Description of License is garbled in License
CSCub73120	3	ils	CUCM 9.x Call Pickup fails if incoming calling party transformation set
CSCsy73190	3	ipma-service	Unable to change the default assistant from Manager UI and Assistant con

Identifier	Severity	Component	Headline
CSCud12752	3	jtapisdk	Get party info length incorrect after drop shareline from conference
CSCue45668	3	licensing	User Licence not uploading successfully on BE3K
CSCue39140	3	perf-counter-lib	Utils diagnose test shows incorrect status for tomcat_memory
CSCud05621	3	rtmt	RTMT version 8.9X and 9.0 still reference the deprecated NetDump utility
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
CSCug55011	3	security	CDR File Transfer Fails with "Unsupported type: PRIVATE KEY" Error
CSCuf20596	3	security	phone authentication with unknown LSC successful
CSCuh75468	4	selinux	2nd change with PWRecovery method displays systax errors with HW servers
CSCue99027	3	ucm-uct	UCT fails to access large CUCM systems
CSCud67624	6	ucm-user-licensing	TelePresence Room license requirements require additional Enhanced
CSCuc02731	6	uri-dialing	Some special character cannot be dialed from phone

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

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

Table 4: Open Caveats for IM and Presence Service Release 9.1(1a)

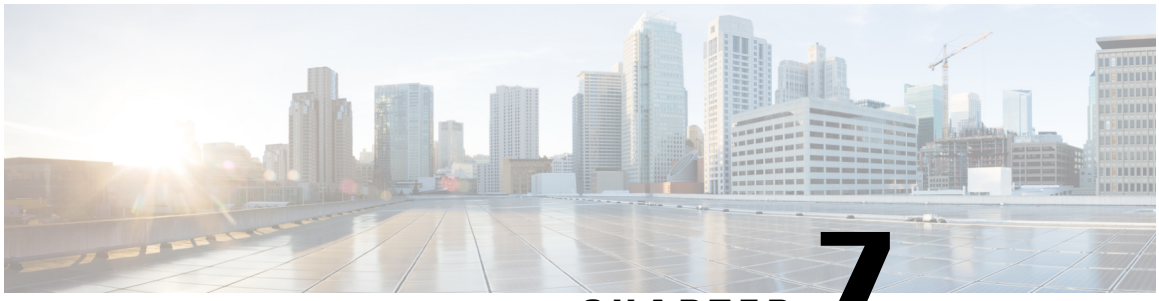
Identifier	Severity	Component	Headline
CSCtw75780	3	bat	Some imported contacts' presence not showing when max contacts size set
CSCtz96671	3	cupxcpconfig	Incorrect restart notification for sub's XMPP fed connection manager

Identifier	Severity	Component	Headline
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	4	security	Setting Admin CLI admin user password returns an incorrect error message
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
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 Release 9.1(2)

The following table lists open caveats that may cause in the latest Enterprise License Manager release. These caveats may also be open in previous releases.

Device	Description	Fix
License Migration Utility	• Now supports manual license upgrades for all Unified Communications Manager versions and Cisco Unity Connection UWL licenses. • Uninstalled DLUs and unregistered license PAKs must be fulfilled and installed prior to Unified Communications Manager upgrade.	• 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) or Release 9.1(2)	Upgrade orders for 9.x do not issue any license PAKs. License version upgrades to 9.x are done through manual license issuance from Cisco Licensing.	To manually upgrade your existing licenses, submit a case to licensing@cisco.com.
Upgrades from Release 9.0(1) to Release 9.1(1) or Release 9.1(2)	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 reissuance to an Enterprise License Manager 9.1(1) license file.	If your license file includes UWL Premium or Advanced UCL, contact Cisco at licensing@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) or 9.1(2) 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 licensing@cisco.com for license file replacement.



CHAPTER 7

Documentation Updates

- License Mac References, page 52
- Administration Guide, page 52
- Call Detail Records Administration Guide, page 57
- CLI Reference Guide, page 60
- Disaster Recovery System Guide, page 60
- Features and Services Guide, page 62
- Installing Cisco Unified Communications Manager, page 68
- Interdomain Federation for IM and Presence Service, page 70
- Partitioned Intradomain Federation for IM and Presence Service, page 71
- Managed Services Guide, page 71
- Real-Time Monitoring Tool Guide, page 72
- Security Guide, page 74
- Serviceability Guide, page 78
- System Guide, page 81
- TCP and UDP Port Usage Guide, page 82
- Upgrade Guide, page 84
- User Options Guide, page 84
- XML Developers Guide, page 84
- Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service, page 85
- Online Help for Cisco Unified Communications Manager, page 86
- Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager, page 86

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.

Conference Bridge Section Updates

This documentation update resolves CSCuh66772.

Because Unified Communications Manager 9.1(2) supports only an IP address configuration for Cisco TelePresence MCU, users must be told to add the correct IP address in to the certificate.

The Administration Guide and online help for the entry "Use HTTPS" mentions the following: "For information on how to create a TLS connection between Cisco Unified Communications Manager and Cisco TelePresence MCU, see the Set up a TLS connection with Cisco TelePresence MCU section." This is not related to setting up HTTPS.

The information on TLS and HTTPS is fairly identical. For HTTPS, the IP address of MCU configured on Unified Communications Manager must be configured as Alternate Name in the MCU certificate, because Unified Communications Manager allows only an IP address to be configured for MCU on the conference bridge page.

The existing section on TLS setup should be the following: "Set up a TLS and HTTPS connection with Cisco Telepresence." Also, on the MCU page help for HTTPS, the information should be changed to the following: "For information on how to create TLS and HTTPS connection between Cisco Unified Communications Manager and Cisco Telepresence MCU, see the Set up a TLS and HTTPS connection with Cisco Telepresence section. "

The Cisco Unified CM Administration online help erroneously contains links for TelePresence Conductor and TelePresence Exchange System.

Disable Early Media on 180 Correction

This documentation update resolves CSCup68350.

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

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

This documentation update resolves CSCur62680.

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

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

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

Hostnames in IPv4 and IPv6 Environments

This documentation update resolves CSCun74975.

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

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

Hub_None Location Correction

This documentation update resolves CSCuu40700.

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

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

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.

Phone Support for Multilevel Precedence and Preemption

This documentation update resolves CSCvb37715.

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

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

Transmit UTF8 for Calling Party Name Field Correction

This documentation update resolves CSCup45037.

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

locale field, and both the Common Device Configuration record, and the Phone record itself have user locale fields.

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

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

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.

A Server Restart is Required After Uploading a Certificate

This documentation update resolves CSCux67134.

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

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

ILS Restictions for Directory URIs

This documentation update resolves CSCus74994.

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

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

Cisco Unified IP Phone setup Description Character Length

This documentation update resolves CSCut08307.

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

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

Correction in Software Conference Bridge Maximum Audio Streams

This documentation update resolves CSCuu44805.

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

Call Detail Records Administration Guide

FAC and CMC Code is not Captured in CDR

This documentation update resolves CSCus91749.

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

FAC

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

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

FAC Example 2

Blind conference using FAC:

1. Call from 136201 to 136111.
2. 136111 answers and speaks for a few seconds.

3 136201 presses the **Conference** softkey and dials 136203.

4 The user is prompted to enter the FAC code and the user enters 124. FAC code 124 is configured as level 1 and given a name as Forward_FAC.

5 While 136203 is ringing, 136201 presses the **Conference** softkey to complete the conference.

6 136203 answers the call.

7 The three members in the conference talk for sometime.

8 136111 hangs up, leaving 136201 and 136203 in the conference. Since there are only two participants in the conference, the conference feature will join these two directly together and they talk for a few seconds.

FieldNames	Orig Call CDR	Setup Call CDR	Conference CDR 1	Conference CDR 2	Conference CDR 3	Final CDR
globalCallID_callId	60015	60016	60015	60015	60015	60017
origLegCallIdentifier	23704372	23704374	23704373	23704372	23704376	23704377
destLegCallIdentifier	23704373	23704376	23704381	23704380	23704382	23704378
callingPartyNumber	136201	136201	136111	136201	136203	136201
origCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
finalCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
lastRedirectDn	136111	136203	136201	136201	136201	136203
origCause_Value	393216	0	16	393216	393216	0
dest_CauseValue	393216	0	393216	393216	393216	16
authCodeDescription		Forward_FAC				
authorizationLevel	0	1	0	0	0	0
Duration	18	0	37	37	32	38
authorizationCode		124				

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

CMC Example 2

Blind conference using CMC :

1 Call from 136201 to 136111.

2 136111 answers and speaks for a few seconds.

3 136201 presses the **Conference** softkey and dials 136203.

4 The user is prompted to enter the CMC code and the user enters 125. CMC code 125 is configured as level 1 and is given a name as Forward_CMC.

5 While 136203 is ringing, 136201 presses the **Conference** softkey to complete the conference.

6 136203 answers the call.

7 The three members in the conference talk for sometime.

8 136111 hangs sup, leaving 136201 and 136203 in the conference. Since there are only two participants in the conference, the conference feature will join these two directly together and they talk for a few seconds.

FieldNames	Orig Call CDR	Setup Call CDR	Conference CDR 1	Conference CDR 2	Conference CDR 3	Final CDR
globalCallID_callId	60025	60026	60025	60025	60025	60027
origLegCallIdentifier	23704522	23704524	23704523	23704522	23704526	23704527
destLegCallIdentifier	23704523	23704526	23704531	23704530	23704532	23704528
callingPartyNumber	136201	136201	136111	136201	136203	136201
origCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
finalCalledPartyNumber	136111	136203	b00105401002	b00105401002	b00105401002	136203
lastRedirectDn	136111	136203	136201	136201	136201	136203
origCause_Value	393216	0	16	393216	393216	0
dest_CauseValue	393216	0	393216	393216	393216	16
authCodeDescription		Forward_CMC				
authorizationLevel	0	1	0	0	0	0
Duration	20	0	32	32	25	48
authorizationCode		125				

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

CLI Reference Guide

ILS Troubleshooting Tips Corrections

This documentation update resolves CSCun09203.

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

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

utils ils find route is an invalid command.

Show perf query counter Command Output

This documentation update resolves CSCuo70238.

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

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

Disaster Recovery System Guide

Cygwin SFTP Servers

This documentation update resolves CSCus64397.

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

For Cygwin to function properly as your backup SFTP server, you must add the following lines to the `sshd_config` file:

The cipher key: ciphers aes128-cbc

The Unified Communications Algorithm: KexAlgorithms diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1

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 5: 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

Bulk Certificate Import May Cause Phones To Restart

This documentation update resolves CSCun32117.

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

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

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.

Calling Party Normalization Restriction

This documentation update resolves CSCuo56960.

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

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

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

Centralized Proxy TFTP File Signature Verification Failure

This documentation update resolves CSCud18710.

When a phone requests a common file from a central or proxy TFTP server and that file has a common name such as `ringlist.xml.sgn` or is a locale file, the TFTP server sends its own local copy of the file instead of the file from the home cluster of the phone. The phone rejects the file due to a signature verification failure because the file has the signature of the TFTP server's local cluster, which does not match the Initial Trust

List (ITL) of the phone. To resolve this issue, you can either disable Security By Default (SBD) for the phone or perform the bulk certificate export procedure to make the Trust Verification System (TVS) return a success when the phone verifies a signature from a different cluster. See the procedure in the "Default Security Setup" section of the *Cisco Unified Communications Manager Security Guide* for performing a bulk certificate export when migrating IP phones between clusters. To disable Security by Default, see the procedure to update the ITL file for IP Phones in the *Cisco Unified Communications Manager Security Guide*.

Cisco Unified Communications Manager Sends INVITE Message to VCS

This documentation update resolves CSCuv22205.

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

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

Client Matter Codes, Forced Authorization Codes, and Failover Calls

This documentation update resolves CSCuv41976.

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

CMCs and FACs do not support failover calls.

Configuring OpenAM Section

This documentation update resolves CSCup44177.

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

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

- Login module
- J2EE agent

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

Procedure

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

Step 2 Select the **Access Control** tab.

A list of one or more access control realms appears.

Step 3 Click **Top Level Realm**.

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

An additional set of configuration tabs appears.

Step 4 Select the **Subjects** tab.

Step 5 Click **New**.

A list of fields containing user details appears.

Step 6 Enter data for the following fields:

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

  Note Do not change this default password.
- **User Status**: Select the **Active** radio button.

Step 7 Click **OK**.

The system creates a "demo" user successfully.

Corrected License Report Update Interval

This documentation update resolves CSCuv84693.

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

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

Corrections for the Immediate Divert Feature

This documentation update resolves CSCun20448.

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

Configure Immediate Divert

Step 6

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

Step 7

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

System requirements for Immediate Divert

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

- Cisco Unified Communications Manager 6.0 or later
- ***Table 6: 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 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.

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.

Incorrect Report for Device Mobility

This documentation update resolves CSCuv20382.

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

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

Jabber Devices Count as Registered Devices

This documentation update resolves CSCur73944.

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

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

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

New Audio Files for Music On Hold

This documentation update resolves CSCut93896.

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

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

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

1. After you upload the new audio file to replace the old one, find the audio source ID you want to change under the **Music On Hold Audio Source Configuration** window.
2. Select a different audio source file, such as the default **SampleAudioSource** and then click **Save**.

3 Switch the source file back to your file you want to use, and then click **Save**.

4 Reset the Music On Hold server so that the changes take effect.

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.

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.

Video Capabilities and Enhanced Location Call Admission Control

This documentation update resolves CSCut20187.

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

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

Call Pickup Restriction

This documentation update resolves CSCuy92491.

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

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

4000 Series Integrated Services Routers do not support Mobile Voice Access

This documentation update resolves CSCvb33454.

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

Mobile Voice Access (MVA)

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

Installing Cisco Unified Communications Manager

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*.

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.

Interdomain Federation for IM and Presence Service

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

This documentation update resolves CSCtw47643.

You cannot install a server-client authentication certificate that is signed by a Microsoft certificate authority (CA) into the local computer store of a Microsoft Office Communications Server (OCS) running Windows 2008. Attempting to copy the certificate from the current user store to the local computer store fails with the error message that the private key is missing.

To resolve this issue, perform the following procedure:

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

FIPS Not a Requirement for Federated Connections with LYNC 2010 Servers

This documentation update resolves CSCui45519.

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

Use TLS for Static Routes

This documentation update resolves CSCui01368.

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

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.

Managed Services Guide

SNMP Limits

This documentation update resolves CSCuv32781.

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

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

Unified Communications Manager Alarms

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

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

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

Real-Time Monitoring Tool Guide

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

This documentation update resolves CSCuq28511.

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

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

Incorrect Default Value for LogPartitionLowWaterMarkExceeded Alert

This documentation update resolves CSCuq39087.

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

Table 7: Default Configuration for the LogPartitionLowWaterMarkExceeded RTMT Alert

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

LowAvailableVirtualMemory Threshold Value is Incorrect

This documentation update resolves CSCuu72197.

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

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.

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**.

Security Guide

Bulk Certificate Import May Cause Phones To Restart

This documentation update resolves CSCun32117.

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

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

Incorrect Configuration Example for ASA Router

This documentation update resolves CSCuv20903.

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

The following procedure contains the correct example.

Procedure

Step 1 Complete the local configuration.

a) Configure network interface.
Example:

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

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

Example:

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

c) Configure the DNS.
Example:

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

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

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

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

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

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

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

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

- Generate a self-signed certificate.

  Example:

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

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

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

  Example:

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

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

- Register the generated certificate with Cisco Unified Communications Manager.

  Example:

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

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

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

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

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

IP Phone SSL VPN not Supported on Third Party Firewalls

This information applies to CSCun49156.

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

Replace ASA Certificate on AnyConnect VPN Phone

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

Procedure

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

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

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

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

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

Step 6 Reset the VPN phones.

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

Step 8 Activate the new ASA certificate on the ASA.

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

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

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

Secure and Nonsecure Indication Tone

This documentation update resolves CSCuq04604.

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

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

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

This documentation update resolves CSCuz68165.

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

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

ITL File Size Limitation

This documentation update resolves CSCvb44649.

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

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

Serviceability Guide

AXL Web Service Requirement for ICSA HA

This documentation update resolves CSCup00956.

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

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

Cisco CAR DB Service

This documentation update resolves CSCup98304.

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

Cisco CAR DB Service

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

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

CAR Database Update

This documentation update resolves CSCuv12448.

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

Cisco Certificate Change Notification Service

This documentation update resolves CSCup84785.

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

Cisco Certificate Change Notification Service

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

Cisco SOAP-CallRecord Service

This documentation update resolves CSCup98302.

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

Cisco SOAP-CallRecord Service

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

Platform Administrative Web Service

This documentation update resolves CSCup84833.

The following service is incorrectly added to the " Feature Services" section in the *Cisco Unified Communications Manager Serviceability Guide* and online help. This service belongs to the "Network Services" section.

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.

SNMP Limits

This documentation update resolves CSCuv32781.

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

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

IM and Presence Security Best Practice

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

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

SOAP-Diagnostic Portal Database Service

This documentation update resolves CSCuq22399.

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

SOAP-Diagnostic Portal Database Service

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

Error in SYSLOG-MIB Parameters

This documentation update resolves CSCux59529.

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

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

System Guide

Call Transfer to Hunt Pilot Restriction

This documentation update resolves CSCuw57732.

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

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

Insufficient Information About Third-Party Restrictions

This documentation update resolves CSCvc16660.

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

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

Video Resolution Support for SIP Phones

This documentation update resolves CSCuf57901.

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

- If the session level bandwidth is greater than 800 Kbps and the imageattr[640 x 480] line in the SDP exists, then VGA is used.

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

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

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

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

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

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

Time of Day routing not Implemented for Message Waiting Indicator

This documentation update resolves CSCva13963.

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

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

TCP and UDP Port Usage Guide

Corrected Port Information

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 8: 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

Missing Information about Common Service Port 8006

This documentation update resolves CSCuy48628.

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

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

Upgrade Guide

Adding a New Subscriber Causes Device Reset

This documentation update resolves CSCub12922.

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

Special Characters in LDAP Password Cause Upgrade Failure

This documentation update resolves CSCuj59481.

If the LDAP profile configure on IM and Presence Service nodes has a password that contains special characters, the upgrade may fail. Cisco recommends that you create a password that uses alpha-numeric characters only.

User Options Guide

The Fast Dial User Option is Not Supported

This documentation update resolves CSCuf57054.

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

XML Developers Guide

Serviceability XML API Doc in Error

This documentation update resolves CSCum01216.

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

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

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

Domain Name Change for Cisco Unified Communications Manager

This documentation update resolves CSCuw76028.

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

Update Domain Name for Cisco Unified Communications Manager

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

Before You Begin

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

Procedure

Step 1 Log in to Command Line Interface.

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

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

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

Step 5 Repeat this procedure for all cluster nodes.

What to Do Next

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

Online Help for Cisco Unified Communications Manager

Incorrect Description for Destination Number

This documentation update resolves CSCux74230.

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

Directory Number Field Description Updated

This documentation update resolves CSCuy28500.

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

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

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

Retrieve Chat Rooms on a Replaced Node

This documentation update resolves CSCuy96037.

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

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