Release Notes for Cisco Unified Communications Manager Release 10.5(2) and IM and Presence Service Release 10.5(2b)

First Published: 2014-12-08

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-32173-02

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

© 2017 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Introduction to Release 10.5(2)** 1

About Release Notes 1

IM and Presence Service, Release 10.5(2b) 2

Documentation for Release 10.5(2) 2

Upgrades 2

Supported Web Browsers 2

CHAPTER 2 **Upgrades** 5

Software Versions 5

Software Upgrades 5

Important Notes about Upgrades 6

Cisco Unified Communications Manager Upgrades to Release 10.5(2) using Prime Collaboration Deployment 6

IM and Presence Service and Cisco Unified Communications Manager Upgrade to 10.5(2) 6

No Configuration During Upgrades 7

Preupgrade COP File 7

Refresh Upgrades to Cisco Unified Communications Manager Release 10.5(2)SU2+ 8

Upgrades to IM and Presence Service, Release 10.5(2b) 9

Upgrades from IM and Presence Service 10.0(1) Export Unrestricted 9

OS Admin Account Required for CLI-Initiated IM and Presence Upgrades 9

CHAPTER 3 **New and Changed Features** 11

Information Assurance Features 11

Login Attempt Information 11

User Interface Changes 12

End User Settings 12

New Service Parameter 13

Update to Default Threshold for Failed Logon Attempts 13

New System Roles 13
Control of Security Status 14
New to the User Interface 14
Touchless Installation for Virtual Machine 15
Automatic Sequencing of Touchless Server 15
Answer File Generator 15
Predefined Cluster Configurations (AFG Process) 16
Touchless Installation Configuration Task Flow 16
Generate and Download a Floppy Image 16
Install a Cluster 17
Install a Cluster When the Dynamic Cluster Configuration Timer is Enabled 17
Install the Cluster When the Dynamic Cluster Configuration Timer is Not Enabled 18
IM and Presence Service Integration 19
CLI Commands 20
set network cluster subscriber details 20
set network cluster subscriber dynamic-cluster-configuration 21
show network cluster 21
unset network cluster subscriber details 21
unset network cluster subscriber dynamic-cluster-configuration 22
show logins unsuccessful 22
Support Removed for utils vmtools status 23
Single Sign-On Updates 23
Increased Capacity of IP Voice Media Streaming Application and Expanded MOH Audio Source 23
Performance Impact of Media Devices with Services 24
Configuration Limitations for Capacity Planning 26
Configure Music On Hold Audio Source 27
AES 256 Encryption Support for TLS and SIP SRTP 28
AES 256 and SHA-2 Support in TLS 29
AES 256 Support in SRTP SIP Call Signaling 30
Cisco Unified Communications Manager Requirements 30
Interactions and Restrictions 31
Remote Control of TelePresence Product Specific Configurations 31
IM and Presence Service Stream Management 31

IM and Presence Service Managed File Transfer 32

CHAPTER 4 **Important Notes 35**

Call Control 35

SIP IPv6 Calls Fail When Using UDP 35

Disaster Recovery System 35

DRS Restore of Failed IM and Presence Service Database Publisher Node Requires DRS Restore of Cisco Unified Communications Manager Publisher Node 35

DRS Restore Status Shows Failed Due to a DB Restore Failure Condition 36

Features and Services 36

6900 Series Phones Fail to Connect When Accessing Personal or Corporate Directories 36

USB Music on Hold Fixed Audio Adapter is not Supported 36

IM and Presence Service 37

Cisco XCP Router Service Fails to Start 37

Presence Engine Core on Startup 37

Availability and IM Broken Between Publisher and Subscriber After Upgrade 37

Enable or Disable FIPS for IM and Presence Service 37

Installation 38

Floppy Image Needed for Unattended Installations 38

Installation Warnings 38

Interoperability 39

Cisco Unified Mobility Disclaimer 39

Failure to Add Unified CM Cluster for Collaboration Edge with TLS Verify Enabled If Unified CM Shares Certificate 39

Failover Interoperability with Cisco Jabber Clients 39

Feature Limitations when Interoperating with Expressway 40

IM and Presence Service Interoperability with Cisco Telepresence Video Communication Server (VCS Control) 42

XCP Restart Notification from Cisco Telepresence Video Communication Server (VCS Control) 42

Media Resources 42

Transcoder is Inserted for SIP Phones During a Midcall Codec Change 42

Miscellaneous 43

Change Perfmon Counter File Size Parameters in RTMT 43

Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets 43

Devices Reset with Certificate Regeneration 43
G.729 Millisecond Packet Size Limitation 43
Intermittent HTTP 500 Error with an SAML SSO Test 43
MGCP IOS Gateway From PSTN Does Not Support Connected Address in ISDN Notify 43
Oauth Token Never Expires 44
Object ID in show hardware CLI Command Is Incorrect 44
Perfect Forward Secrecy is not Supported in IPsec Configuration 44
RTP Library Components Update for 64 bit 44
RtpLib Callbacks Usage 45
Softkeys Not Working for 7936 47
Speed Dial in Self Care Portal 47
TFTP File Size Limit 47

CHAPTER 5 Caveats 49
Bug Search Tool 49
Resolved Caveats 50
Open Caveats 50
Caveats 50
Open Caveats for Cisco Unified Communications Manager, Release 10.5(2) 50
Open Caveats for IM and Presence Service, Release 10.5(2) 52

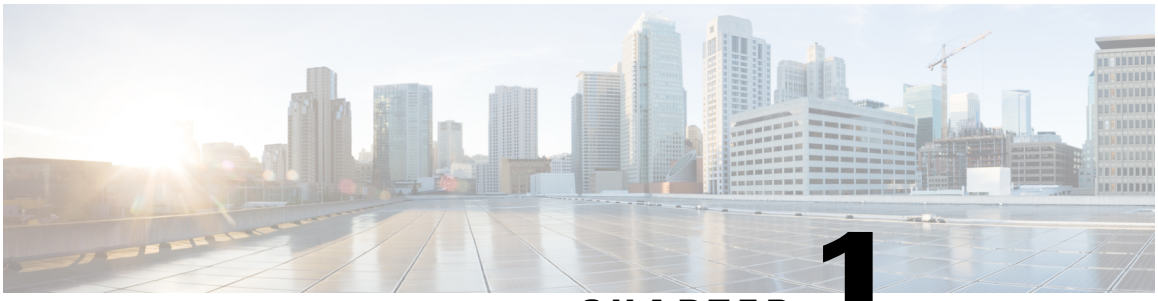
CHAPTER 6 Documentation Updates 55
Administration Guide 56
Cisco Unified IP Phone setup Description Character Length 56
Correction in IPv6 Address Field 56
Correction in Software Conference Bridge Maximum Audio Streams 57
Directory Number Field Description Updated 57
Directory Number Line Behavior in Cisco Unified Communications Manager 57
Disable Early Media on 180 Correction 58
Extension Mobility Now Supports Device Owners 58
Forbidden String When Configuring Directory Number Alert Names 58
Hostname and IP Address Field Can Contain a Fully Qualified Domain Name 58
Hostnames in IPv4 and IPv6 Environments 59
Hub_None Location Correction 59

ILS Data Sync to be Delayed Until after DB Replication is Completed 59
ILS Restictions for Directory URIs 59
Incorrect External Call Control Profile Field Description 59
Incorrect Information about Deleting Route Patterns 60
Incorrect Note about User Locales 61
Incorrect Time Period Example 61
Insufficient Information about Call Control Agent Profile Fields 61
Line Group Deletion Correction 62
Location Menu Path 62
Maximum Hunt Timer Restriction 62
Missing Information for Allow Multiple Codecs in Answer SDP 63
Phone Support for Multilevel Precedence and Preemption 63
Remove Resource Priority Namespace List Field from SIP Profile Settings 63
Self-Provisioning Application Requires Phone Model with Security By Default 63
Service Profiles and Device Owner User IDs 64
SIP Trunk Fields SIP Trunk Status and SIPTrunk Duration 64
Synchronize Trunks and Gatekeeper Sections Are Not Valid 65
Transmit UTF8 for Calling Party Name Field Correction 65
Insufficient Information About Automatic Fallback 65
UDS in Remote Cluster Service Configuration is Not Supported 66
A Server Restart is Required After Uploading a Certificate 66
LDAP Authentication Correction 66
Authenticate with Multiple LDAP Domains 67
Certificate Monitor Frequency Interval 67
Bulk Administration Guide 67
Bulk Administration Character Length 67
Bulk Administration Gateway Deletion Changes 68
EMCC Device Calculation in the Bulk Administration Tool 68
Removed Fields in Delete User Device Profiles Custom Configuration 68
TAPS and Cisco UCCX with a Standard License 69
Call Detail Records Administration Guide 69
Four New Fields in Call Details Record 69
FAC and CMC Code is not Captured in CDR 71
CLI Reference Guide 73
ILS Troubleshooting Tips Corrections 73

Show perf query counter Command Output 74
Support Removed for utils vmtools status 74
Disaster Recovery System Guide 74
Supported SFTP Servers 74
Features and Services Guide 75
Add or Update Hosted DN Pattern Through CSV File 75
Call Pickup Group Visual Notification Does Not Support Localization 75
Calling Party Normalization Restriction 76
Cisco Unified Communications Manager Sends INVITE Message to VCS 76
Client Matter Codes and Force Authorization Codes Not Supported on Cisco Jabber 76
Client Matter Codes, Forced Authorization Codes, and Failover Calls 76
Corrected License Report Update Interval 77
Corrections for the Immediate Divert Feature 77
Cisco Unified Mobility Documentation Changes 78
Default Partitions 78
Incorrect Multicast Music On Hold Restriction 79
Force Authorization Codes Not Supported on Cisco Jabber 79
Incorrect Report for Device Mobility 79
Jabber Devices Count as Registered Devices 79
Locations Media Resource Audio Bit Rate Policy Service Parameter Limitation 80
Music On Hold and Native Call Queuing Behavior 80
Remote Destination and Auto Answer 80
Restart Intercluster Lookup Service 80
SAF Forwarder and Requesting Service Arrow Keys Removed 80
SAML Not Enabled after Upgrade on Web Dialer 81
SAML SSO Authentication LDAP Attribute for User ID Setting 81
Video Capabilities and Enhanced Location Call Admission Control 81
Call Pickup Restriction 81
JTAPI Developers Guide 82
MeetMe: Unsupported JTAPI Feature 82
Unsupported CTI Events From SIP Phones 82
Managed Services Guide 83
SNMP Limits 83
Online Help for Cisco Unified Communications Manager 83
Backup Device Limit Incorrect in Disaster Recovery System Online Help 83

Incorrect Description for Destination Number 83
Directory Number Field Description Updated 83
Remote Destination Configuration Page In the OLH Needs To Be Updated 84
OS Administration Guide 84
Documentation Update for Certificate Monitor Configuration 84
Add CA Signed CAPF Root Certificate to Trust Store 84
Real-Time Monitoring Tool Guide 85
Analyze Call Path Tool does not Work with Non-English Language 85
Incorrect Default Value for LogPartitionLowWaterMarkExceeded Alert 85
Incorrect Minimum Rate for Monitoring a Performance Counter 85
New LowAvailableVirtualMemory Threshold 86
FQDN Support to Display Hostnames in RTMT 86
RTMT Mail Server Procedure Correction 86
Security Guide 86
Bulk Certificate Import May Cause Phones To Restart 86
Replace ASA Certificate on AnyConnect VPN Phone 87
Secure and Nonsecure Indication Tone 87
Incorrect Configuration Example for ASA Router 88
Enable Password Persistence 90
Resync Bandwidth Option is Removed 90
CNF File Encryption Is Not Supported by Default on 6901 and 6911, Cisco IP Phones 90
ITL File Size Limitation 91
Serviceability Guide 91
Cisco CAR DB Service 91
Cisco Certificate Change Notification Service 91
Cisco IP Phone Service Removed from CM Services 92
Cisco SOAP-CallRecord Service 92
Delayed Initialization after IP Manager Assistant Service Restart 92
Platform Administrative Web Service 92
Self Provisioning IVR Service 93
SNMP Limits 93
IM and Presence Security Best Practice 93
SOAP-Diagnostic Portal Database Service 93
Error in SYSLOG-MIB Parameters 94
Minimize Disk Space utilized by Log Files 94

System Guide 94
Call Transfer to Hunt Pilot Restriction 94
Email IDs on the Active Directory Server 94
LDAP Directory Support 95
Bandwidth Calculations 95
Insufficient Information About Adding a New ILS Hub 95
Insufficient Information About Third-Party Restrictions 96
Time of Day routing not Implemented for Message Waiting Indicator 96
TAPI Developers Guide 97
Unsupported CTI Events from SIP Phones 97
TCP and UDP Port Usage Guide 97
Missing Information about TCP Port 22 97
Missing Information about TCP Port 5555 97
Missing Information about Common Service Port 8006 98
Upgrade Guide 98
Disable or Postpone LDAP Synchronization During an Upgrade 98
InterCluster Peer-User and Admin-CUMA Application User Roles Deprecated 98
Unified CM 10.0 Upgrade Process Correction 99
Configuration and Administration Guide for IM and Presence Service 99
UDS Directory Supported with Directory URI IM Addressing 99
Retrieve Chat Rooms on a Replaced Node 99
Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service 99
Domain Name Change for Cisco Unified Communications Manager 99
Update Domain Name for Cisco Unified Communications Manager 100



CHAPTER 1

Introduction to Release 10.5(2)

- About Release Notes, page 1
- Documentation for Release 10.5(2), page 2
- Upgrades, page 2
- Supported Web Browsers , page 2

About Release Notes

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

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

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

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

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

IM and Presence Service, Release 10.5(2b)

This document also applies to IM and Presence Service, Release 10.5(2b). There was a respin of the IM and Presence Service 10.5(2a) release to address high severity defects. Release 10.5(2b) contains resolutions for the following high severity defects:

- CSCut16613 - Configuring IM&P fails silently due to memory leak in XCP Config Mgr svc
- CSCus27395 - December 2014 - NTPd.org Vulnerabilities
- CSCus69785 - Evaluation of glibc GHOST vulnerability - CVE-2015-0235
- CSCur67798 - Cisco XCP Connection Manager service crashes during stream resumption

Release 10.5(2b) also contains the resolution to CSCus27634, which was included in Release 10.5(2a).

Note If you are currently running IM and Presence Service, Release 10.5(2) or 10.5(2a), it is recommended that you upgrade to Release10.5(2b). For details, see Upgrades to IM and Presence Service, Release 10.5(2b), on page 9.

Documentation for Release 10.5(2)

For complete information about this release, refer first to these Release Notes for information about new and changed features in this release and then refer to the *Documentation Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 10.5(2)* at the following URL:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/docguide/10_5_2/CUCM_BK_D6D433CE_00_CUCM-documentation-guide-1052.html

Upgrades

For information about upgrading, as well as requirements for hardware and software, see the *Install and Upgrade Guides* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

Supported Web Browsers

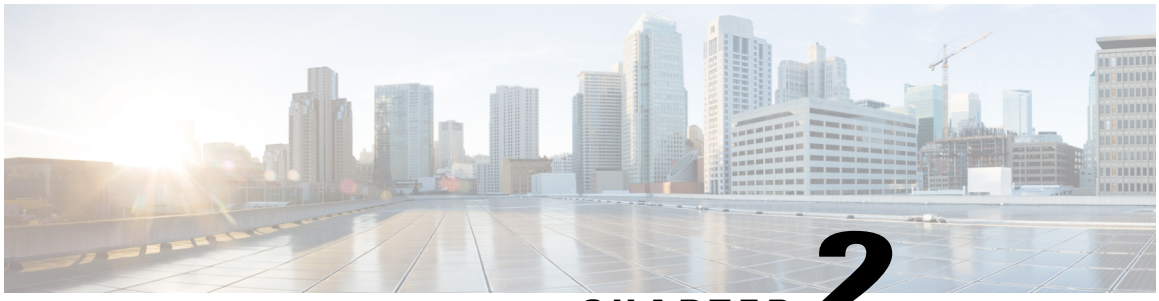
Release 10.5(2) supports the following web browsers:

- Internet Explorer 10 and 11
- Firefox v32.0
- Chrome v37.0
- Safari v7

Note For maximum security when accessing your system, we recommend that you use Google Chrome.

The above web browsers can be used on the following Cisco Unified Communications Manager user interfaces:

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- CDR Analysis and Reporting
- Disaster Recovery System
- Cisco Unified Communications Self Care Portal



CHAPTER 2

Upgrades

- Software Versions, page 5
- Software Upgrades, page 5
- Important Notes about Upgrades, page 6

Software Versions

Software Version for Cisco Unified Communications Manager Release 10.5(2)

- These release notes are based on the following software version: 10.5.2.10000-5.

Software Version for IM and Presence Service Release 10.5(2)

- These release notes are based on the following software version: 10.5.2.20000-1.

Software Upgrades

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

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

For information about the upgrade process and related tasks, see the *Upgrade Guide for Cisco Unified Communications Manager* at:

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-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.

Important Notes about Upgrades

Cisco Unified Communications Manager Upgrades to Release 10.5(2) using Prime Collaboration Deployment

Follow these guidelines if you are using Cisco Prime Collaboration Deployment to upgrade Cisco Unified Communications Manager to release 10.5(2):

- PCD upgrades or non-PCD upgrades from release 10.0(1) or 10.5(1) are supported. Migrations from 10.0(1) or 10.5(1) using Prime Collaboration Deployment are not supported. For definitions of migrations and upgrades, see the latest release of the *Cisco Prime Collaboration Deployment Administration Guide*. For additional details, see CSCur99079.
- Before upgrading to release 10.5(2), you must download and install the COP file ciscocm.version3-keys.cop.sgn on every node in the cluster prior to upgrading. This Cisco Options Package (COP) file has the RSA keys that are required to validate the upgrade.
- If you are upgrading from 6.1(5), 7.x, 8.x, 9.x, or 10.x, you must disable the time synchronization between the VM instance and the ESXi. To disable the time synchronization issue, follow the instructions at the following URL:

  http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1189

  An alternative method is to configure the ESXi server and the Cisco Unified Communications Manager publisher node to point to the same NTP server.

  This resolves CSCur94973.

You can download COP files from the following location on cisco.com: **Downloads** > **Products** > **Unified Communications** > **Call Control** > **Unified Communications Manager (CallManager)** > **Cisco Unified Communications Manager Version 10.5**

IM and Presence Service and Cisco Unified Communications Manager Upgrade to 10.5(2)

Note You must upgrade Cisco Unified Communications Manager to Release 10.5(2) before you upgrade the IM and Presence Service nodes.

If you want to upgrade IM and Presence Service from Release 10.5(1) (or earlier) to 10.5(2), you must also upgrade Cisco Unified Communications Manager to Release 10.5(2).

Similarly, if you upgrade Cisco Unified Communications Manager from Release 10.5(1) (or earlier) to 10.5(2), you must also upgrade IM and Presence Service to Release 10.5(2).

IM and Presence Service Release 10.5(2) is compatible only with Cisco Unified Communications Manager Release 10.5(2).

No Configuration During Upgrades

Do not perform any configuration tasks during the upgrade process.

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

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

Preupgrade COP File

If you are upgrading to Cisco Unified Communications Manager Release 10.5(1), or later, from a release earlier than Cisco Unified Communications Manager Release 10.0(1), you must download and install ciscocm.version3-keys.cop.sgn on every node in the cluster. This Cisco Options Package (COP) file has the RSA keys that are required to validate the upgrade. Missing RSA-3 keys will result in status errors in the Software Installation/Upgrade window of the Cisco Unified Operating System Administration interface.

If you are upgrading to Cisco Unified Communications Manager Release 8.6 or later from a release earlier than Cisco Unified Communications Manager Release 8.5, you must download and install the latest ciscocm.refresh_upgrade_version.cop.sgn on every node in the cluster.

For detailed steps about COP file installation and complete upgrade procedures, see the *Upgrade Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

Note If the ciscocm.version3-keys.cop.sgn file is not installed, then software validation will fail even if the md5sum value of the ISO is correct.

To find COP files on Cisco.com, navigate to **Support** > **Downloads** > **Cisco Unified Communications Manager Version <version>** > **Unified Communications Manager/CallManager/Cisco Unity Connection Utilities**.

Note Cisco Prime Collaboration Deployment does not automatically install the required COP file before upgrade. You must create a task in Cisco Prime Collaboration Deployment to install the COP file before the upgrade. For more information, see the *Cisco Prime Collaboration Deployment Administration Guide*.

Verify that you have the correct COP file installed with the following commands:

```
admin:show version active

Active Master Version: 8.5.1.10000-26

Active Version Installed Software Options:
```

```
ciscocm.version3-keys.cop

ciscocm.refresh_upgrade_v1.5.cop.sgn

admin:
```

IM and Presence Service

You must also install the ciscocm.version3-keys.cop.sgn cop file before you upgrade to IM and Presence Service Release 10.5(1), or later, from any release earlier than 10.0(1). This COP file is necessary for all upgrades from pre-10.0(1) to 10.5(1) and later.

Upgrade from Cisco Unified Presence 8.5(4)

For upgrades from Cisco Unified Presence 8.5(4), you must install two COP files in the following order before you begin the upgrade:

1. Install the refresh upgrade COP file, cisco.com.cup.refresh_upgrade_v<latest_version>.cop. You can download this COP file from Cisco.com.
2. Install the RSA-3 key COP file, ciscocm.version3-keys.cop.sgn.

Downgrade to Cisco Unified Presence 8.6(3)

Cisco Unified Presence Releases 8.6(4) and later do not support the Cisco Presence Engine database. If you upgrade from Release 8.6(3) to Release 10.5(1) and you subsequently want to revert to Release 8.6(3), you must install a COP file that will reinstall the Cisco Presence Engine database. The COP filename is ciscocm.cup.pe_db_install.cop and you can download it from Cisco.com.

Note In a multinode environment, you must install the ciscocm.cup.pe_db_install.cop COP file on every node in the cluster after you switch back to Release 8.6(3).

Refresh Upgrades to Cisco Unified Communications Manager Release 10.5(2)SU2+

Currently, the *Upgrade Guide for Cisco Unified Communications Manager and IM and Presence Service* instructs administrators performing a refresh upgrade of Cisco Unified Communications Manager nodes that they must both upgrade and switch versions on the publisher node before they begin to upgrade subscriber nodes.

As of Cisco Unified Communications Manager Release 10.5(2)SU2 and higher, administrators have the option of holding off switching versions until after all cluster nodes are upgraded. For this case, the revised order would be:

1. Upgrade the Unified Communications Manager publisher node.
2. Upgrade the Unified Communications Manager subscriber nodes.
3. Switch the publisher node to the upgraded partition.
4. Switch the subscriber nodes to the upgraded partition.

Note You can switch the subscriber nodes to the upgraded partition either all at once, or one at a time, depending on your site requirements.

For Cisco Unified Communications Manager Release 10.5(2)SU2 and higher, administrators can apply this optional version switching sequence to the Refresh Upgrade task lists in the "Upgrades Overview" chapter of the *Upgrade Guide for Cisco Unified Communications Manager and IM and Presence Service*.

Upgrades to IM and Presence Service, Release 10.5(2b)

If you are upgrading to IM and Presence Service, Release 10.5(2b) then you must use the following set of files:

- `Bootable_UCSInstall_CUP_10.5.2.21900-4.sgn.iso`

  `bootable ISO image; md5 hash: 3a62b5beff66f50137717c3ab370dbbe`

- `Bootable_UCSInstall_CUP_UNRST_10.5.2.21900-4.sgn.iso`

  `bootable ISO image (unrestricted); md5 hash: 8229548df0012fe60ad0c1b30eefcc5e`

- `UCSInstall_CUP_10.5.2.21900-4.sgn.iso`

  `non-bootable ISO image (upgrades only); md5 hash: 5efbcc6de8dcadaf6de2ff7220126627`

- `UCSInstall_CUP_UNRST_10.5.2.21900-4.sgn.iso`

  `non-bootable ISO image (upgrades only, unrestricted); md5 hash: 05481ad99189c32dd23722f6226248d9`

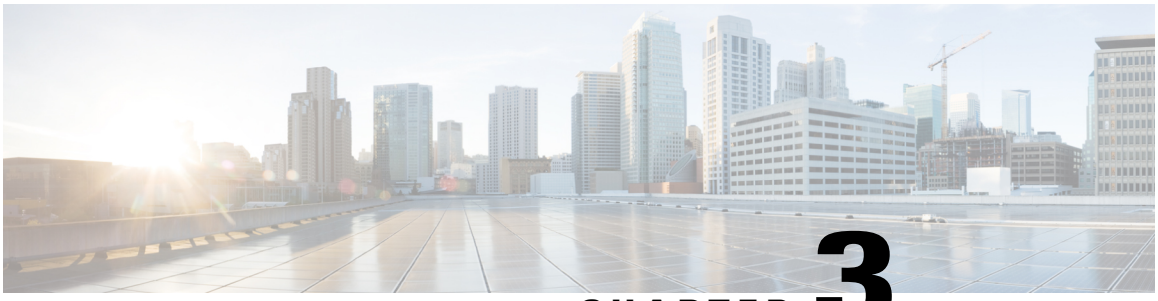
Upgrades from IM and Presence Service 10.0(1) Export Unrestricted

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

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

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

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



CHAPTER 3

New and Changed Features

- Information Assurance Features, page 11
- Update to Default Threshold for Failed Logon Attempts, page 13
- New System Roles, page 13
- Control of Security Status, page 14
- Touchless Installation for Virtual Machine, page 15
- Single Sign-On Updates, page 23
- Increased Capacity of IP Voice Media Streaming Application and Expanded MOH Audio Source, page 23
- AES 256 Encryption Support for TLS and SIP SRTP, page 28
- Remote Control of TelePresence Product Specific Configurations, page 31
- IM and Presence Service Stream Management, page 31
- IM and Presence Service Managed File Transfer, page 32

Information Assurance Features

This section describes the new Information Assurance features added as part of Cisco Unified Communications Manager Release 10.5(2).

Login Attempt Information

When you log in to web applications for Cisco Unified Communications Manager or IM and Presence Service, the main application window displays the last successful system login attempt and the last unsuccessful system login attempt for the current user along with the user ID, date, time, and IP address.

The following web applications display the login attempt information:

- Cisco Unified Communications Manager:
  - Cisco Unified CM Administration

- Cisco Unified Reporting
- Cisco Unified Serviceability

- IM and Presence Service
  - Cisco Unified CM IM and Presence Administration
  - Cisco Unified IM and Presence Reporting
  - Cisco Unified IM and Presence Serviceability

You can use the **show logins unsuccessful** CLI command to view login information for the Disaster Recovery System and Cisco Unified OS Administration web applications.

User Interface Changes

In **Cisco Unified CM Administration** under **User Management** > **End User**, the following buttons were added to the **Find and List Users** window:

- **Enable Selected Local User—**The administrator can enable a single user or multiple users in bulk if needed.
- **Disable Selected Local User—**The administrator can disable a single user or multiple users in bulk if needed.

Note The **Enable Selected Local User** and the **Disable Selected Local User** buttons are visible only when the **Disable User Accounts unused for (days)** service parameter value is set to 1 or more days in the Cisco Database Layer Monitor service.

End User Settings

In **Cisco Unified CM Administration**, the following buttons were added in the **End User Configuration** window.

- **Enable Local User—**The administrator can enable a single user if the **User Status** is set to Disabled.

Note This button appears only when the **User Status** is set to Disabled.

- **Disable Local User—**The administrator can disable a single user if the **User Status** is set to Enabled.

Note This button appears only when the **User Status** is set to Enabled.

Note The **Enable Local User** and the **Disable Local User** buttons are visible only when the **Disable User Accounts unused for (days)** service parameter value is set to 1 or more days in the Cisco Database Layer Monitor service.

New Service Parameter

A new service parameter called **Disable User Accounts unused for (days)** was added in the **Service Parameter Configuration** window under the Cisco Database Layer Monitor service. This parameter specifies how often users must authenticate with Cisco Unified Communications Manager to prevent their account from being automatically disabled.

The user account is disabled if the user does not log in to Cisco Unified Communications Manager with their PIN or Password in the number of days that is specified in the **Disable User Accounts unused for (days)** field.

If both the **Disable User Accounts unused for (days)** field and the **Inactive Days Allowed** field in the **Credential Policy Configuration** window are configured, the field that has a lower value takes precedence.

For example: If the **Inactive Days Allowed** field is set to 30 days and the **Disable User Accounts unused for (days)** field is set to 45 days, and the user does not log in to Cisco Unified Communications Manager within 30 days, the user account remains enabled until 45 days but the user will not able to log in.

If the **Disable User Accounts unused for (days)** field is set to 30 days and the **Inactive Days Allowed** field is set to 45 days, and the user does not log in within 30 days to Cisco Unified Communications Manager, the user account is disabled.

Update to Default Threshold for Failed Logon Attempts

With release 10.5(2), the default value for the number of failed logon attempts for both administrator accounts and end user accounts has been changed to five. By default, if an administrator, or an end user, enters an incorrect username and password combination five times, the account is locked.

For end users, you can reconfigure the number of failed logon attempts by assigning a new credential policy in the **End User Configuration** window.

Administrators can reset the administrator password by using the `utils reset_application_ui_administrator_password`.

New System Roles

The following table summarizes the new standard roles and access control groups that come preconfigured on Cisco Unified Communications Manager.

Table 1: Standard Roles, Privileges, and Access Control Groups

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard SSO Config Admin	Allows you to administer all aspects of SAML SSO configuration	
Standard Confidential Access Level Users	Allows you to access all the Confidential Access Level Pages	Standard Cisco Call Manager Administration
Standard CCMADMIN Administration	Allows you to administer all aspects of CCMAdmin system	Standard Cisco Unified CM IM and Presence Administration
Standard CCMADMIN Read Only	Allows read access to all CCMAdmin resources	Standard Cisco Unified CM IM and Presence Administration
Standard CUReporting	Allows application users to generate reports from various sources	Standard Cisco Unified CM IM and Presence Reporting

For more information about the Roles and User Groups, see *Cisco Unified Communications Manager System Guide* .

Control of Security Status

For releases earlier than Cisco TelePresence Multipoint Control Unit (MCU) Release 4.5 and Cisco TelePresence Conductor Release XC2.3, Cisco Unified Communications Manager provides the call-security icon, according to security levels that are configured for the Cisco Unified Communications Manager servers and the conference participants. With Cisco TelePresence MCU Release 4.5 and Cisco TelePresence Conductor Release XC2.3, SIP video conferencing resources can determine the security status of video conferences and indicate the status to the participants. Sometimes, for Ad hoc and Meet-Me conferences, the security status determined by the SIP video conferencing resources conflicts with the security status determined by Cisco Unified Communications Manager. With Release 10.5(2), you can configure a SIP Cisco TelePresence MCU or a Cisco TelePresence Conductor to control the display of call-security icon in a video conference.

New to the User Interface

In Cisco Unified CM Administration, under **Media Resources** > **Conference Bridge**, an **Allow Conference Bridge Control of the Call Security Icon** check box is added to the **Device Information** area. This check box is unchecked by default. You must check the check box to allow the MCU or the Conductor to control the display of the call-security icon. You can leave the check box unchecked if you want Cisco Unified Communications Manager to control the display of the call-security icon.

This check box is displayed only if you select the **Conference Bridge Type** as **Cisco Telepresence MCU** or **Cisco TelePresence Conductor**.

Touchless Installation for Virtual Machine

Previous releases of Cisco Unified Communications Manager cluster environment required you to install the publisher node first before you proceed to install the subscriber nodes. You had to install the subscriber nodes after adding them to the server page of the publisher node and repeat the same procedure for each subscriber node. With the touchless installation feature, the subscriber nodes are configured dynamically along with the publisher node during their installation.

Touchless installation is a new feature in Cisco Unified Communications Manager. This feature makes the installation process seamless and promotes simplified cluster installation. The touchless installation proceeds without the requirement to provide any subscriber details in the installation wizard. Subscribers are not dependent on the installation of the publisher. This feature has the following benefits:

- No manual intervention and scheduling during the deployment of a new cluster.
- No manual entry of each subscriber and simplifies the addition of new subscribers to an existing cluster.
- No requirement to wait until the publisher node is active.

Automatic Sequencing of Touchless Server

Automatic sequencing is an approach that facilitates the installations of both the publisher node and the subscriber nodes in a cluster at the same time without manual intervention. Subscriber nodes wait for the publisher node to complete its installation, and then get added to the database of the publisher node to continue with their own installation. After the publisher node is installed, it authenticates each subscriber. After authentication, each subscriber node receives a signal from the publisher node and the installation of that subscriber node continues automatically.

Initiate automatic sequencing by enabling the **Dynamic Cluster Config Enable** timer checkbox and providing a value in the **Dynamic Cluster Config Timer** field. You can enable this timer by using one of the following methods:

- Answer File Generator (AFG) tool.
- Command line interface (CLI) command on the Cisco Unified Communications Manager publisher node.

Answer File Generator

Use the Answer File Generator (AFG) tool (http://www.cisco.com/web/cuc_afg/index.html) to generate the answer files or floppy image files for configuration. These files include `clusterConfig.xml` and `platformConfig.xml` files. The `clusterConfig.xml` file is a new file in Cisco Unified Communications Manager Release 10.5(2).

Start the virtual machine on which you mounted the ISO and floppy image to start the Cisco Unified Communications Manager installation. No manual intervention is required during installation of a standalone node or a cluster.

In a cluster environment, you can install both the publisher node and the subscriber nodes simultaneously. Sometimes, the installation of the subscriber nodes can stop during the installation of the publisher node. In

this case, after the publisher node installation is complete, it generates a signal for the subscriber nodes to continue their installation.

Predefined Cluster Configurations (AFG Process)

With the implementation of this feature, the Answer File Generator (AFG) tool generates the `clusterConfig.xml` file along with the existing the `platformConfig.xml` file. If you provide the details of subscriber nodes to the AFG tool, the `clusterConfig.xml` file includes those details. After the Cisco Unified Communications Manager publisher is installed, it reads the `clusterConfig.xml` file and if the publisher finds any subscriber nodes, it adds them to its processnode tables. Adding the subscribers to processnode tables eliminates the need to wait for the Cisco Unified Communications Manager publisher to finish its installation, and then manually add the subscribers on the server page. The entire installation process occurs automatically.

Touchless Installation Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Generate and Download a Floppy Image, on page 16.	Generate the floppy image using the Answer File Generator tool. The floppy image consists of two precreated answer files—`platformConfig.xml` and `ClusterConfig.xml` files that are downloaded automatically when you download the floppy image.
Step 2	Install a Cluster, on page 17 • Install a Cluster When the Dynamic Cluster Configuration Timer is Enabled, on page 17 • Install the Cluster When the Dynamic Cluster Configuration Timer is Not Enabled, on page 18	Install a cluster in one of the following ways: • Install the publisher node and subscriber nodes with no manual intervention by enabling the **Dynamic Cluster Config Enable** timer. • Install the subscriber nodes when you do not enable the **Dynamic Cluster Config Enable** timer while generating the answer files.

Generate and Download a Floppy Image

The Cisco Unified Communications Answer File Generator web application generates the answer files for Cisco Unified Communications installations. These precreated answer files are `platformConfig.xml` and `ClusterConfig.xml` files and are included in the floppy image.

Perform the following procedure to generate and download the floppy image:

Procedure

Step 1 Log in to the Cisco Unified Communications Answer File Generator application.

Step 2 Enter details in the **Clusterwide Configuration** section.

Step 3 Enter details for the primary node in the **Primary Node Configuration** section.

Step 4 To enable Dynamic Cluster Configuration, from the **Dynamic-Cluster-Configuration** section, enable the **Dynamic Cluster Config Enable** timer check box and enter a value in the **Dynamic Cluster Config Timer** field.
Specify a value from 1 to 24 for this field, where the number indicates hours.

Note If you do not enable the **Dynamic Cluster Config Enable** timer and specify its value in the **Dynamic Cluster Config Timer** field while you to generate the answer files, you will have to enable this timer later when the publisher node gets installed automatically but the subscriber nodes are waiting for installation. Then, you will have to add the subscriber nodes manually so that their installation occurs automatically.

Step 5 Enter details for the secondary node in the **Secondary Node Configuration** section.

Step 6 In the **List of Secondary Nodes** list box, select **Add Secondary Node**.
The node that you add as secondary node appears in this list box.

Step 7 Repeat Steps 5 and 6 for additional secondary nodes.

Step 8 Click **Generate Answer Files**.
A dialog box appears showing the details for the primary node, the secondary node, and the `clusterConfig` file.

Step 9 In the **Communications Answer File Generator** dialog box, follow the download instructions, and then click the **Download File** button to download the answer files to your computer.

Install a Cluster

Depending on whether you enabled the **Dynamic Cluster Config Enable** timer in the Answer File Generator tool or not, you can choose one of the following ways to install a cluster:

- Install the publisher node and subscriber nodes with no manual intervention by enabling the **Dynamic Cluster Config Enable** timer. See Install a Cluster When the Dynamic Cluster Configuration Timer is Enabled, on page 17.
- Install the subscriber nodes when you do not enable the **Dynamic Cluster Config Enable** timer while generating the answer files. See Install the Cluster When the Dynamic Cluster Configuration Timer is Not Enabled, on page 18.

Install a Cluster When the Dynamic Cluster Configuration Timer is Enabled

Before You Begin

Enable the **Dynamic Cluster Config Timer** field by one of the following ways:

- Click the **Dynamic Cluster Config Enable** timer checkbox and enter a value in the **Dynamic Cluster Config Timer** field in the Answer File Generator tool. For details, see Step 4 of the Generate and Download a Floppy Image, on page 16 procedure.
- Enter the **set network cluster subscriber dynamic-cluster-configuration** {*default* | *no. of hours*} CLI command.

Procedure

Step 1 Mount the floppy image on the virtual machine.

Note If the virtual machine is Cisco Unified Communications Manager publisher node, then the floppy image contains both the `platformConfig.xml` and `ClusterConfig.xml` files. However, if the virtual machine is Cisco Unified Communications Manager subscriber node or IM and Presence publisher node or subscriber nodes, the floppy image contains only the `platformConfig.xml` file.

For details on how to create a floppy a new virtual floppy image, see http://docwiki.cisco.com/wiki/How_to_Use_the_AFG_with_the_Virtual_Floppy_Drive.

Step 2 Start the publisher node and all subscriber nodes.

Publisher node and subscriber nodes get installed automatically with no manual intervention. Each subscriber node gets automatically added to the publisher through the automatic sequencing approach.

Install the Cluster When the Dynamic Cluster Configuration Timer is Not Enabled

If you do not enable the **Dynamic Cluster Config Timer** field in the Answer File Generator tool, the publisher node gets installed automatically. However, the subscriber nodes will be waiting for their installation.

To avoid the waiting time of the subscriber nodes so that the cluster installation continues, perform one of following tasks:

- From the Cisco Unified Communications Manager, select the **Web Interface** and click the **Server** tab and add the subscriber nodes manually.
- Enable the **Dynamic Cluster Config Timer** field from the CLI of the publisher node with the new CLI command that is available in Cisco Unified Communications Manager Release 10.5(2)**—set network cluster subscriber dynamic-cluster-configuration** {*default* | *no. of hours*}. After you enable this timer, the subscriber nodes get added to the publisher automatically and the installation of the subscriber nodes proceeds.

Note

- If you need to add one or more subscribers as specified for the publisher node, you can add them while you generate the `platformconfig.xml` file. You have to specify the publisher node and the subscriber nodes. If the **Dynamic Cluster Config Timer** timer is still active, subscribers get automatically added to the publisher and the installation of the subscriber nodes continues.
- This feature has no limitation on predefining the number of subscriber nodes that you need to add to a publisher node.

Use the WinImage tool to create the disk images. Mount the ISO images through VMware ESXi.

Before You Begin

Place the floppy image at datastore from where it is accessible to virtual machine for mounting.

Procedure

Step 1 Start the virtual machine to start the cluster installation.

Step 2 From the **VM** menu, choose **Edit settings** to mount the floppy image that you have created from the Answer File Generator tool.
The **Virtual Machine Properties** dialog box appears.

Step 3 From the available hardware list, select **Floppy drive 1**.

Step 4 In the **Device Type** section, select **Use the existing floppy image in the database**, and then click **Browse** to navigate to the floppy image.

Step 5 Click **OK**.
The floppy image is attached.

Step 6 Select the **CD/DVD Drive 1** > **Connect to ISO image on local disk** option from the toolbar and choose **CD/DVD Drive1** > **Connect to ISO image on a datastore**, navigate to the data store to select the installer ISO image, and click **OK**.
The ISO image is attached and the installation starts.

Step 7 (Optional) If you want to test the media before the installation, click **OK** in the **Disc Found** message box, or click **Skip** to skip testing the media before the installation.
The installation proceeds without any manual intervention. The publisher is installed and the subscribers are added to the publisher.

IM and Presence Service Integration

This feature supports heterogeneous cluster-wide installation that includes Cisco Unified Communications Manager and IM and Presence Service nodes. The concept and installation process for IM and Presence Service is same as the installation process for Cisco Unified Communications Manager in a cluster.

From the AFG tool, check the **Dynamic Cluster Config Timer** check box, select IM and Presence Service, and enter the details for Cisco Unified Communications Manager publisher node, IM and Presence Service publisher node, and IM and Presence Service subscriber details (if any). Then, AFG tool generates the `clusterConfig.xml` file along with `platformConfig.xml` file for each node. You can use this `clusterConfig.xml` file only with Cisco Unified Communications Manager publisher node along with `platformConfig.xml` file that is generated for this node. For all other nodes, only `platformConfig.xml` file is used.

Answer File Generator (AFG) saves the domain name of IM and Presence Service publisher in the `clusterConfig.xml` file along with the existing details.

The integration of Cisco Unified Communications Manager with IM and Presence includes the following tasks:

- The IM and Presence Service publisher is added to the processnode table with domain name after the installation of Cisco Unified Communications Manager.

- Cisco Unified Communications Manager and IM and Presence Service nodes are added to the processnode table using the IP address, if available.
- When you add the IM and Presence Service publisher through CLI, the domain is added.

CLI Commands

Cisco Unified Communications Manager Release 10.5(2) includes the following new CLI commands:

Note For details on CLI commands, see the *Command Line Interface Guide for Cisco Unified Communications Solutions* and the *Installing Cisco Unified Communications Manager*.

set network cluster subscriber details

Use this command to add subscriber to the processnode or appserver table when Tomcat Webserver is server down and GUI is inaccessible.

set network cluster subscriber details *servertype hostname ip domainname*

Syntax Description

Parameter	Description
servertype	Choose one of these products for this parameter—Cisco Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection. This field is mandatory.
hostname	The hostname of the node that you add to the cluster. The hostname is supported on the same domain. This field is mandatory.
ip	The IPv4 address of the node that you add to the cluster. This field is mandatory for IM and Presence publisher and Cisco Unity Connection.
domainname	The domain name of the IM and Presence Service publisher. This field is mandatory for IM and Presence publisher.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to Cisco Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection

set network cluster subscriber dynamic-cluster-configuration

Use this command to enable the Dynamic Cluster Configuration on the publisher. Use this command to specify the duration in which you can add subscriber nodes to the publisher server table. The addition of subscriber nodes is authenticated immediately and those nodes need not wait for the publisher details during the installation of the subscriber nodes.

set network cluster subscriber dynamic-cluster-configuration {**default | no. of hours**}

Syntax Description

Parameter	Description
default	Enables the Dynamic Cluster Configuration for 24 hours.
no. of hours	Specifies a value from 1 to 24 hours.

Command Modes

Administrator (admin)

Requirements

Applies to Cisco Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection

show network cluster

This command is enhanced to show the remaining timer value when you enable Dynamic Cluster Configuration.

show network cluster

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to Cisco Unified Communications Manager, IM and Presence Service on Cisco Unified Communications Manager, and Cisco Unity Connection

unset network cluster subscriber details

This command shows the message that you need to delete a subscriber node from the GUI instead of the command prompt.

unset network cluster subscriber details

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to Cisco Unified Communications Manager, IM and Presence Service on Communications Manager, and Cisco Unity Connection

Message to delete the subscriber from GUI

```
admin: unset network cluster subscriber details
Please use the Cisco Unified Communications Manager on the first node.
Navigate to System > Server and click “Find”.
   Unable to del: NULL
Executed command unsuccessfully.
```

unset network cluster subscriber dynamic-cluster-configuration

This command disables Dynamic Cluster Configuration on the publisher. The value of **Dynamic Cluster Configuration** option is set to zero on publisher.

unset network cluster subscriber dynamic-cluster-configuration

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to Cisco Unified Communications Manager, IM and Presence Service on Cisco Unified Communications Manager, and Cisco Unity Connection

show logins unsuccessful

Use this command to list recent unsuccessful login attempts to the following web applications:

- On Cisco Unified Communications Manager
  - Disaster Recovery System
  - Cisco Unified OS Administration
- On IM and Presence Service
  - IM and Presence Disaster Recovery System
  - Cisco Unified IM and Presence OS Administration

show logins unsuccessful [*number*]

Syntax Description

Parameters	Description
number	Specifies the number of most recent logins to display. The default is 20.

Command Modes

Administrator (admin)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to Cisco Unified Communications Manager and IM and Presence Service

Support Removed for utils vmtools status

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

Single Sign-On Updates

The following SAML SSO - related enhancements are introduced in Cisco Unified Communications Manager, Release 10.5(2).

Export/Import of SSO Metadata

In **Cisco Unified Communications Manager Administration**, under **System** > **SAML Single Sign-On**, the **Export All Metadata** button is enabled by default, regardless of whether the SAML SSO state is set to active.

Enable SAML SSO

The following note was added to the Enable SAML SSO procedure in the *Features and Services Guide*.

Note After you click **Import IdP Metadata** and click **Next**, a status message appears in the **SAML Single Sign-On Configuration** window. It displays information to either skip or continue further with steps to upload the server metadata to the IdP.

Increased Capacity of IP Voice Media Streaming Application and Expanded MOH Audio Source

Cisco IP Voice Media Streaming application is installed automatically when you install Cisco Unified Communications Manager. Activate this application to enable the Music On Hold (MOH) feature.

With this release, the capacity of Cisco Unified Communications Manager to support unique and concurrent MOH audio sources, while the Music On Hold service is running on the MOH server, is increased from 51 to 501. The MOH audio sources are numbered from 1 to 501 with the fixed MOH audio source remaining at the number 51.

The fixed MOH device cannot use an audio source that connects through a USB MOH device, because Cisco Unified Communications Manager does not support USB when running on VMware. Use of the fixed MOH USB device is not supported on VMware. However, provision the external sound device for use with deployments that utilize Cisco Unified Survivable Remote Site Telephony (SRST) multicast MOH.

You can configure each MOH audio source to use a custom announcement as an initial greeting and/or an announcement that is played periodically to callers who are hearing the music. Cisco Unified Communications Manager provides 500 custom announcements that you can use on one or multiple MOH audio sources. These announcements are not distributed between the Cisco Unified Communications Manager servers within a cluster. You have to upload these custom announcement files to each server that provides the MOH and announcement services. You must also upload each custom music file for MOH audio sources to each server.

Performance Impact of Media Devices with Services

The Cisco IP Voice Media Streaming application runs as a service for four media devices—annunciator (ANN), software conference bridge, Music On Hold (MOH), and software media termination point. Activate this service on a Cisco Unified Communications Manager server as coresident with call processing. When you activate this service, ensure that you configure these media devices for limited capacity to avoid any impact on the call processing. The default settings for the media devices are defined based on this coresident operation. You can adjust these settings by reducing the use of one or more media devices to increase other settings.

For example, if you are not using software media termination point devices, you can choose the **Run Flag** setting for the SW MTP to **False**, select **System** > **Service Parameters** > **Cisco IP Voice Media Streaming App service** > **MTP Parameters** , and add the **MTP Call Count** setting to **Media Resource** > **MOH Server** > **Maximum Half Duplex Streams** configuration. Depending on the call traffic, you can modify the default settings. However, monitor the server performance activity for CPU, memory, and IO wait. For higher capacity clusters, such as the ones using 7500 user OVA configuration, it is possible to increase the default media device settings for Call Count by 25%.

For installations where you expect high usage of the media devices, such as Music On Hold, or where high call volumes require higher number of media connections, activate the Cisco IP Voice Media Streaming application service on one or more of the Cisco Unified Communications Manager servers which do not have call processing activated. Activating this service limits the impact of media device usage to other services, such as call processing. Then, you can increase the configuration settings for maximum number of calls for the media devices.

When you activate Cisco IP Voice Media Streaming application as co-resident with Cisco Unified Communications Manager service, it can impact call processing performance. To increase the capacity settings for Music On Hold or annunciator from the default settings, it is suggested to activate Cisco IP Voice Media Streaming application on a server without activating Cisco Unified Communications Manager.

The CPU performance is impacted by MOH when active callers are on hold or when multicast MOH audio streams are configured.

Table 2: General Performance Results

Configuration Notes	CPU Performance
Dedicated MOH server, 1000 held calls, 500 MOH sources with greeting and periodic announcements.	25–45% (7500 user OVA configuration)
Native call queuing with dedicated MOH server and annunciator server, 1000 queued calls, 500 MOH sources with greeting and periodic announcements. An annunciator can play up to 300 simultaneous greeting announcements.	25–45% (7500 user OVA configuration)
Dedicated MOH server, 500 held calls, 500 MOH sources with greeting and periodic announcements.	15–35% (7500 user OVA configuration)

Table 3: Extrapolated Recommendations

Configuration	Recommendation Limit
When Cisco IP Voice Media Streaming application is co-resident with Cisco Unified Communications Manager on 2500 OVA (moderate call processing).	MOH: 500 held callers, 100 MOH sources, and 48 to 64 annunciator callers.
When Cisco IP Voice Media Streaming application is a dedicated server on 2500 OVA.	MOH: 750 held callers, 250 MOH sources, and 250 annunciator callers.
When Cisco IP Voice Media Streaming application is co-resident with Cisco Unified Communications Manager on 7500/10K OVA (moderate call processing).	MOH: 500 held callers, 250 MOH sources, and 128 annunciator callers.
When Cisco IP Voice Media Streaming application is a dedicated server on 7500/10K OVA.	MOH: 1000 held callers, 500 MOH sources, and 300-700 annunciator callers (with 1 MOH codec). **Note** Reduce annunciator to 300 for two MOH codecs.

Note These recommendations are specific to MOH/ANN devices. If you combine these devices with the software media termination point (MTP) and call forward busy (CFB) devices, reduce the limits to provide streams.

Configuration Limitations for Capacity Planning

The Cisco IP Voice Media Streaming application and Self Provisioning IVR services use a media kernel driver to create and control Real-time Transfer Protocol (RTP) streams. This media kernel driver has a capacity of 6000 streams. These streams allow the media devices and IVR to make resource reservations.

These reservations are based on the following capacity calculations:

Media Device	Capacity
Annunciator	(Call Count service parameter) * 3 Where 3 indicates total of receiving (RX) and transmitting (TX) calls for endpoint and 1 for .wav file.
Software Conference Bridge	(Call Count service parameter) * 2 Where 2 indicates total streams of RX and TX endpoints.
Software Media Termination Point	(Call Count service parameter) * 2 Where 2 indicates total streams of RX and TX endpoints.
Music On Hold	((Maximum Half Duplex Streams) * 3) + (501 * 2 * [number of enabled MOH codecs]) Where: • (Maximum Half Duplex Streams) is a configuration setting on the MOH device configuration administration web page. • 3 indicates total steams of RX, TX, and greeting announcement .wav file. • 501 indicates the maximum number of Music On Hold (MOH) sources. • 2 indicates music .wav stream and possible multicast TX stream. • [number of enabled MOH codecs] is based on how many MOH codecs are enabled in the Cisco IP Voice Media Streaming application service parameters.
Self Provisioning IVR Service	(500 * 2) Where 500 indicates callers, and 2 indicates total streams from RX and TX streams.

Hence, to enable MOH to support a maximum of 1000 callers, use the following equation: `1000 * 3 + 501 * 2 * 1 = 4002` driver streams with one enabled codec and `1000 * 3 +501 * 2 * 2 = 5004` with two enabled codecs. Reduce the remaining devices and deactivate the Self Provisioning IVR service to limit total reservations to 6000, which allows the MOH device to make these reservations. It may also require that you do not activate the Self Provisioning IVR service on the same server with Cisco IP Voice Media Streaming application.

If configuration settings of the media devices exceed the capacity of the media device driver, the media devices that register with the device driver first will be able to reserve their required stream resources. The media devices that register later are restricted to fewer than requested stream resources. The later registered media devices result in logging some alarm messages and automatically reducing the call count for the restricted media device.

Note A media kernel driver with a capacity of 6000 streams might not support that many simultaneous media device connections.

Configure Music On Hold Audio Source

Perform the following procedure to add or update a Music On Hold audio source, to associate an existing audio source with an audio stream number, or to upload a new custom audio source.

Note If a new version of an audio source file is available, perform the update procedure to use the new version.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Media Resources** > **Music On Hold Audio Source**. The **Find and List Music On Hold Audio Sources** window appears.

Step 2 Enter search criteria to update an existing audio source. To list all records in the database, ensure that the dialog box is empty. Click **Find**.

Step 3 Click **Add New** to add a new Music On Hold audio source.

Step 4 Configure the fields in the **Music On Hold Audio Source Configuration** window.

Note

- For the Audio Stream Number, choose from a list of available MOH source numbers that are not already provisioned. You can provision Audio source number 51 in the MOH Fixed Audio Source menu.
- The MOH Audio Source File drop-down list displays all the MOH source files that have been uploaded and are available for assignment to an MOH Audio Stream Number.
- The MOH Audio Source Name is available to provide a description for this MOH Audio Source Number.
- The Initial Announcement is optional and the drop-down list shows the available announcements. You can use the Announcements menu to add new custom greeting announcements or change the audio .wav file that is associated with an announcement.
- If you have to use the MOH Audio Source with the Native Call Queuing feature, the Initial Announcement may be configured to be played before routing to a hunt member. Use the **Played before routing to Hunt Member** option in the Native Call Queuing feature by using an Annunciator. If you select the **Play when call is queued** option for configuring the Initial Announcement or if you are not using the MOH Audio Source with Native Call Queuing, the initial announcement is played to the queued or held caller by the MOH device when the caller is queued or placed on hold.
- Use the **Periodic Announcement** option to choose an announcement to be played on a periodic basis while callers are listening to the MOH Audio Source File.
- Use the **Locale Announcement** configuration to choose which language to be used for the announcements if you have provisioned multiple language announcements. A MOH Audio Source supports only one language (locale).

Step 5 Click **Save**.
The list box at the bottom of the window shows the new Music On Hold audio source. The MOH Audio Source File Status pane shows the MOH audio translation status for the added source.

AES 256 Encryption Support for TLS and SIP SRTP

Cisco Collaboration Solutions use Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) for signaling and media encryption. Currently, Advanced Encryption Standard (AES) with a 128-bit encryption key is used as the encryption cipher. AES also uses Hash-based Message Authentication Code Secure Hash Algorithm-1 (HMAC-SHA-1) as the authentication method. These algorithms cannot effectively scale to meet the required changing security and performance needs. To meet escalating security and performance requirements, the algorithms and protocols for encryption, authentication, digital signatures, and key exchange in Next-Generation Encryption (NGE) are developed. Also, AES 256 encryption support is provided instead of AES 128 for TLS and Session Initiation Protocol (SIP) SRTP that supports NGE.

With Cisco Unified Communications Manager Release 10.5(2), the AES 256 encryption support for TLS and SIP SRTP is enhanced to focus on AES 256 cipher support in signaling and media encryption. This feature is useful for the applications that run on Cisco Unified Communications Manager to initiate and support TLS 1.2 connections with the AES-256 based ciphers that conform to SHA-2 (Secure Hash Algorithm) standards and is Federal Information Processing Standards (FIPS) compliant.

This feature has the following requirements:

- The connection that the SIP trunk and SIP line initiates.
- The ciphers that Cisco Unified Communications Manager supports for SRTP calls over SIP line and SIP trunk.

AES 256 and SHA-2 Support in TLS

The Transport Layer Security (TLS) protocol provides authentication, data integrity, and confidentiality for communications between two applications. TLS 1.2 is based on Secure Sockets Layer (SSL) protocol version 3.0, although the two protocols are not compatible with each other. TLS operates in a client/server mode where one side acts as a server and the other side acts as a client. SSL is positioned as a protocol layer between the Transmission Control Protocol (TCP) layer and the application to form a secure connection between clients and servers so that they can communicate securely over a network. To operate, TLS requires TCP as the reliable transport layer protocol.

In Cisco Unified Communications Manager Release 10.5(2), AES 256 and SHA-2 (Secure Hash Algorithm-2) support in TLS 1.2 is an enhancement to handle the connection that is initiated by the SIP Trunk and the SIP line. The supported ciphers, which are AES 256 and SHA-2 compliant, are listed as follows:

- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256—The cipher string is ECDH-RSA-AES128-GCM-SHA256.
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384—The cipher string is ECDH-RSA-AES256-GCM-SHA384.

where:

- TLS is Transport Layer Security
- ECDH is Elliptic curve Diffie–Hellman, which is an algorithm
- RSA is Rivest Shamir Adleman, which is an algorithm
- AES is Advanced Encryption Standards
- GCM is Galois/Counter Mode

In addition to the newly-supported ciphers, Cisco Unified Communications Manager Release 10.5(2) continues to support TLS_RSA_WITH_AES_128_CBC_SHA. The cipher string of this cipher is AES128-SHA.

Note

- The Cisco Unified Communications Manager certificates are based on RSA.
- In Cisco Unified Communications Manager 10.5(2), Cisco Endpoints (phones) do not support the above mentioned new ciphers for TLS 1.2.
- With AES 256 and SHA-2 (Secure Hash Algorithm-2) support in TLS 1.2 enhancement in Cisco Unified Communications Manager 10.5(2), the default key size for Certificate Authority Proxy Function (CAPF) is increased to 2048 bits.

AES 256 Support in SRTP SIP Call Signaling

Secure Real-time Transport Protocol (SRTP) defines the methods of providing confidentiality and data integrity for both Real-time Transport Protocol (RTP) voice and video media and their corresponding Real-time Transport Control Protocol (RTCP) streams. SRTP implements this method through the use of encryption and message authentication headers. In SRTP, encryption applies to the payload of the RTP packet only, and not to the RTP header. However, message authentication applies to both the RTP header and the RTP payload. Also, SRTP indirectly provides protection against replay attacks because message authentication applies to the RTP sequence number within the header. SRTP uses Advanced Encryption Standards (AES) with a 128-bit encryption key as the encryption cipher. It also uses Hash-based Message Authentication Code Secure Hash Algorithm-1 (HMAC-SHA-1) as the authentication method.

Cisco Unified Communications Manager 10.5(2) supports crypto ciphers for the SRTP calls over SIP line and SIP trunk. These crypto ciphers are AEAD_AES_256_GCM and AEAD_AES_128_GCM, where AEAD is Authenticated-Encryption with Associated-Data, and GCM is Galois/Counter Mode. These ciphers are based on GCM. If these ciphers are present in the Session Description Protocol (SDP), they are treated with higher priority as compared to the AES 128 and SHA-1 based ciphers. Cisco Endpoints (phones) do not support these new ciphers that you add for Cisco Unified Communications Manager 10.5(2) for SRTP.

In addition to the newly supported ciphers, Cisco Unified Communications Manager 10.5(2) continues to support the following ciphers:

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- F8_128_HMAC_SHA1_80

AES 256 encryption is supported in the following calls:

- SIP line to SIP line call signaling
- SIP line to SIP trunk signaling
- SIP trunk to SIP trunk signaling

Cisco Unified Communications Manager Requirements

- Support for TLS Version 1.2 on the SIP trunk and SIP line connections is available.
- Cipher support—TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (cipher string ECDHE-RSA-AES256-GCM-SHA384) and TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (cipher string ECDHE-RSA-AES128-GCM-SHA256)—is available when the TLS 1.2 connection is made. These ciphers are based on GCM and conform to SHA-2 category.
- Cisco Unified Communications Manager initiates TLS1.2 with the TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ciphers. If the peer does not support TLS1.2, then Cisco Unified Communications Manager will fall back to TLS 1.0 with the existing AES128-SHA cipher.
- The SRTP calls over SIP line and SIP trunk support the GCM-based AEAD_AES_256_GCM and AEAD_AES_128_GCM ciphers.

Interactions and Restrictions

- Cisco Unified Communications Manager requirements apply to SIP line and SIP trunk, and basic SIP to SIP calls only.
- The device types that are based on non-SIP protocols will continue to support the existing behavior with the TLS versions with the supported ciphers. Skinny Call Control Protocol (SCCP) also supports TLS 1.2 with the earlier supported ciphers.
- SIP to non-SIP calls will continue to use AES 128 and SHA-1 based ciphers.

Remote Control of TelePresence Product Specific Configurations

Beginning with Release 10.5(2), Cisco Unified Communications Manager can remotely acquire and manage product specific settings for Cisco TelePresence endpoints on behalf of Cisco TelePresence users.

When a Cisco TelePresence endpoint first registers with Cisco Unified Communications Manager, or if a Cisco TelePresence user modifies their product-specific settings from their endpoint, SIP signaling communicates those settings to the Cisco Unified Communications Manager database and the settings display under the Product-Specific-Configuration Layout heading of the Phone Configuration window.

Once those settings are obtained, Cisco Unified Communications Manager administrators can set and change product-specific settings, including administration passwords, on behalf of Cisco TelePresence users.

To communicate the new settings back to the phone, administrators must reset the phone.

IM and Presence Service Stream Management

Cisco Unified Communications Manager IM and Presence Service Release 10.5(2) supports Stream Management for instant messaging. Stream Management is implemented using the XEP-0198 specification, which defines an Extensible Messaging and Presence Protocol (XMPP) extension for active management of an XML stream between two XMPP entities, including features for stanza acknowledgements and stream resumption. For more information about XEP-0198, see the specification at http://xmpp.org/extensions/xep-0198.html.

If there is a temporary loss of communication between IM and Presence Service and Cisco Jabber, Stream Management ensures that any instant messages that are sent during the communications outage are not lost. A configurable timeout period determines how such messages are handled:

- If Cisco Jabber reestablishes communication with IM and Presence Service within the timeout period, the messages are resent.
- If Cisco Jabber does not reestablish communication with IM and Presence Service within the timeout period, the messages are returned to the sender.
- Messages that are sent after the timeout period lapses are stored offline and delivered when Cisco Jabber resumes communication with IM and Presence Service.

Administrators can enable Stream Management on a cluster-wide basis. Use the following Cisco XCP Router service parameters to configure Stream Management.

Service Parameter	Description
Enable Stream Management	Enables or disables Stream Management cluster-wide. The default setting is Enabled.
Stream Management Timeout	The maximum number of seconds that a session will wait before the stream is resumed and the message is resent. If connection to IM and Presence Service cannot be restored within this time frame, the message is returned to the sender. Any messages that are sent after this timeout ends and before Cisco Jabber logs in again with IM and Presence Service are stored offline and resent after relogin. The default setting is 60.
Stream Management Buffer Size	The maximum number of packets that can be stored in a buffer. If Cisco Jabber needs more space than is available in the buffer, IM and Presence Service starts to return messages to senders before they are removed from the buffer to make room for more messages. The default setting is 100.
Acknowledgement Request Rate	The number of stanzas sent by IM and Presence Service before Cisco Jabber is requested to provide the count of the last stanza it received. **Note** A smaller Acknowledgement Request Rate leads to increased network traffic but reduced memory use. The default setting is 5.

To configure these parameters, log in to **Cisco Unified CM IM and Presence Administration**, choose **System** > **Service Parameters** and choose the Cisco XCP Router Service.

IM and Presence Service Managed File Transfer

Managed file transfer (MFT) allows an IM and Presence Service client, such as Cisco Jabber, to transfer files to other users, ad hoc group chat rooms, and persistent chat rooms. The files are stored in a repository on an external file server and the transaction is logged to an external database.

The managed file transfer configuration is specific to this feature and has no impact on the message archiver feature for regulatory compliance.

For more information about the managed file transfer feature, see the *Configuration and Administration Guide of IM and Presence Service on Cisco Unified Communications Manager*.

Two New User Interface Windows

External File Servers

You use the controls in this window to configure an external file server on IM and Presence Service, including the user credentials and connection information.

File Transfer Configuration

You use the controls in this window to configure one of the following options for file transfers on IM and Presence Service: **Disable**, **Peer-to-Peer**, **Managed File Transfer** or **Managed and Peer-to-Peer File Transfer**.

New File Server Troubleshooting Tests

There are seven new tests that are conducted after you complete the deployment of an external file server:

- Verify external file server reachability (pingable)
- Verify that the external file server is listening for connections
- Verify external file server public key is correct
- Verify node public key is configured correctly on the external file server
- Verify external file server directory is valid
- Verify external file server has been mounted successfully
- Verify that free disk space is available on the file server

New Real Time Monitoring Tool Managed File Transfer Alarms

There are three new alarms, two that test connection status between the IM and Presence Service and the external servers and one that tests disk space on the external file server.

- XcpMFTExtFsMountError—Cisco XCP File Transfer Manager has lost its connection to the external file server.
- XcpMFTExtFsFreeSpaceWarn—Cisco XCP File Transfer Manager has detected that the available disk space on the external file server is low.
- XcpMFTDBConnectError—Cisco XCP data access layer was unable to connect to the database.

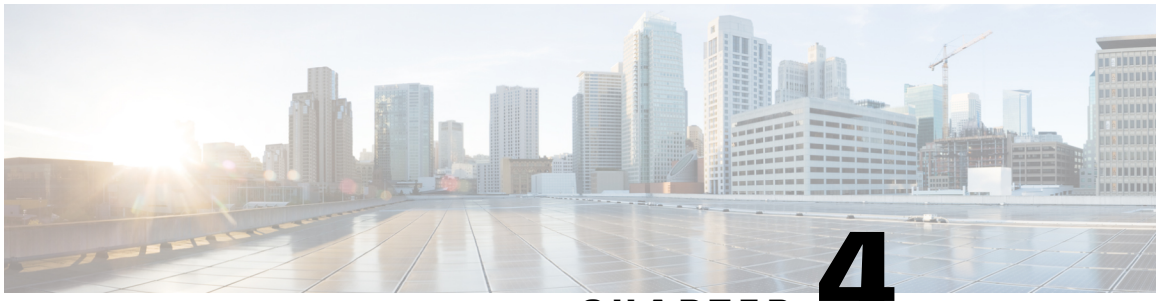
New Real Time Monitoring Tool Managed File Transfer Counters

The Real Time Monitoring Tool (RTMT) now contains one new folder and six new counters for the managed file transfer feature:

- Cisco XCP MFT Counters
    - MFTBytesDownloadedLastTimeslice
    - MFTBytesUpoadedLastTimeslice
    - MFTFilesDownloaded
    - MFTFilesDownloadedLastTimeslice
    - MFTFilesUploaded
    - MFTFilesUploadedLastTimeslice

Deprecated Setting

In the **Service Parameter Configuration** window for the Cisco XCP Router (Active) service, the **Enable file transfer** drop-down list has been removed from the XCP Router Global Settings (Clusterwide) area.



CHAPTER 4

Important Notes

- Call Control, page 35
- Disaster Recovery System, page 35
- Features and Services, page 36
- IM and Presence Service, page 37
- Installation, page 38
- Interoperability, page 39
- Media Resources, page 42
- Miscellaneous, page 43

Call Control

SIP IPv6 Calls Fail When Using UDP

Cisco Unified Communications Manager does not support SIP IPv6 signaling over UDP where the MTU is greater than 1500. To ensure that calls do not fail, change the transport protocol to TCP.

Disaster Recovery System

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

This information applies to CSCuo02154.

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

Workaround

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

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

DRS Restore Status Shows Failed Due to a DB Restore Failure Condition

This information applies to CSCuo56564.

During a DRS restore, you may see a warning message indicating that database replication failed. You can ignore this message. The DRS restore will complete successfully.

Features and Services

6900 Series Phones Fail to Connect When Accessing Personal or Corporate Directories

This information applies to CSCus28530.

6900 series phones may show a connection failed error message when they try to access personal or corporate directories. If you encounter this issue, use the workaround as described here.

Alternatively, you can use the following Cisco Options Package (COP) file: `ciscocm.enable_sslv3-v1.0.cop.sgn`. To obtain the file from https://software.cisco.com/download/navigator.html, navigate to **Downloads** > **Home** > **Products** > **Unified Communications** > **Call Control** > **Unified Communications Manager (CallManager)** > **Unified Communications Manager Version 10.5** > **Unified Communications Manager / CallManager / Cisco Unity COnnection Utilities - COP Files**.

Caution The COP file workaround affects your system security.

USB Music on Hold Fixed Audio Adapter is not Supported

This information applies to CSCun07952.

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

IM and Presence Service

Cisco XCP Router Service Fails to Start

The following information applies to CSCus61289.

Problem:

The Cisco XCP Router service fails to start because of an incorrect internal configuration.

Conditions:

This issue only occurs on an IM and Presence Service server with version 10.5(2) installed, and where the cluster to which it belongs, is interclustered with another Cisco Unified Communications Manager IM and Presence Service cluster. The problem only occurs on the 10.5(2) IM and Presence Service server which initiates the internal router-to-router connection.

Solution:

Restart the Cisco XCP Config Manager service on the 10.5(2) IM and Presence Service server where the Cisco XCP Router service is failing to start. After successfully restarting the Cisco XCP Config Manager service, start the Cisco XCP Router service.

Presence Engine Core on Startup

This information applies to CSCus27634.

After fresh installing or upgrading to IM and Presence Service 10.5.2.10000-9, the Cisco Presence Engine service will not start, and will generate a core file. If you encounter this issue, contact Cisco Technical Assistance Centre (TAC).

Availability and IM Broken Between Publisher and Subscriber After Upgrade

This information applies to CSCuo65513.

After you upgrade a multinode deployment, users that are assigned to one node cannot see the availability of users that are assigned to another node, nor can they send instant messages to users that are assigned to another node.

On the node in which users cannot see the presence of other users, restart the Cisco XCP router.

Enable or Disable FIPS for IM and Presence Service

This documentation update resolves CSCuo56537.

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

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

Installation

Floppy Image Needed for Unattended Installations

This information applies to CSCus0202.

Caution Before you perform an unattended installation of Unified Communications Manager, ensure that a floppy image is mounted with an empty file that is named `POWER_OFF_AFTER_SKIP_INSTALL`. Otherwise, the installation will not proceed and may fail.

Installation Warnings

This information applies to CSCug48896.

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

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

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

Interoperability

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.

Failure to Add Unified CM Cluster for Collaboration Edge with TLS Verify Enabled If Unified CM Shares Certificate

If a Unified Communications Manager cluster is deployed using a multiserver Tomcat certificate, you cannot add the cluster for mobile remote access to a Cisco TelePresence VCS-C/Expressway-C with the TLS verify mode enabled. To add a cluster to the Cisco TelePresence VCS-C/Expressway-C with TLS verify enabled, specify the first node that is mentioned in the Subject Alternative Name (SAN), or change the order of the SAN items making the Unified Communications Manager the first publisher on the SAN list. However, the issue still remains for the IM and Presence Service cluster, and this cluster must be added with TLS verify mode disabled.

Alternatively, you can disable TLS verify mode for both the Unified Communications Manager and IM and Presence Service clusters. This issue is resolved with the release of Cisco TelePresence VCS-C/Expressway-C X8.2.

For details about how to add a Unified Communications Manager cluster to a Cisco TelePresence VCS, see your Cisco TelePresence VCS product documentation.

Failover Interoperability with Cisco Jabber Clients

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

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

Feature Limitations when Interoperating with Expressway

The following table summarizes feature limitations that were observed during the testing of remote TelePresence and Jabber endpoints in deployments that interoperate Cisco Unified Communications Manager with Expressway x8.1.1 or x8.5.

The testing on which this data is based covers the most commonly used features. However, it is not possible to test all scenarios, and as such, Cisco cannot guarantee support for all Cisco Unified Communications Manager features when interoperating with Expressway.

Feature	Endpoint Limitations
Hold/Resume	Audio failure may occur after a held call is resumed in the following cases: • Remote Jabber client calls remote TelePresence endpoint • Remote TelePresence endpoint calls a TelePresence endpoint within the enterprise network
Shared Line	Shared lines are supported in a limited way. Multiple endpoints can share a line, but only one device sharing the line can be behind Expressway. Also, in-call features such as hold/resume work only on the first endpoint that answers. Endpoints sharing the line may not correctly recognize the state of the call. Barge is not supported for shared lines.
Mobility calls	The following Mobility restrictions apply for remote endpoints: • Session handoff not supported • Dial via office is not supported
Secure calls	DTLS signaling is not supported for secure calls.
Phone Security Profile Limitations	When you deploy secured phones in a deployment that interoperates Cisco Unified Communications Manager with Expressway, the number of phone security profiles that you can configure in Cisco Unified Communications Manager is limited by the phone security profile names and the size of the SAN field in the actual certificate. This field cannot exceed 351 characters. Since there will be only one certificate between Cisco Unified Communications Manager and VCS, the SAN field in the certificate must contain the name of each phone security profile and commas separating each name. For example, three phone security profiles named SecProfile1, SecProfile2, and SecProfile3 will use 35 characters.
Conferencing	The following restrictions apply for conferencing: • For conferences that include remote participants, the remote participant cannot be dropped from an active conference. • MeetMe conferencing is not supported with Cisco Jabber.

Feature	Endpoint Limitations
SIP Early Media	Support is offered as follows: • Expressway x8.1.1—Not supported • Expressway x8.5—Limited support (no PRACK), with early media call for basic calls.
Bulk registration	Not supported
Call Park	Not supported
Call Pickup	Not supported
Call Monitoring	Not supported
Call Recording	Not supported
Call Preservation	Not supported
Extension Mobility	Supported with TelePresence endpoints. Not supported with Cisco Jabber.
Key Press Markup Language	Support is offered as follows: • Expressway x8.1.1—Not supported with Expressway x8.1.1. • Expressway x8.5—Limited support for basic calls. Out of dialog KPML is not supported.
Multistreaming	The ability of endpoints to negotiate multiple codecs in the audio channel is not supported.
End to end RSVP	Not supported
Audio codec support	Opus audio codec is not supported.
Video codec support	H.265 is not supported.
Graceful registration	The `x-cisco-graceful-reg` tag for soft client dual registration is not supported.
Roaming	Not supported
Called/Calling Party Transformation CSS	Not supported

IM and Presence Service Interoperability with Cisco Telepresence Video Communication Server (VCS Control)

After you upgrade to IM and Presence Service Release 10.5(2), you must refresh your VCS Control configuration. This procedure is necessary if you have the Mobile and Remote Access feature or XMPP federation deployed.

Procedure

Step 1 On the VCS Control master node, navigate to **Configuration** > **Unified Communications** > **IM and Presence Servers**.

Step 2 Check the check box for each of the IM and Presence Service database publisher nodes.

Step 3 Click the **Refresh Servers** button.

Step 4 If necessary reload the page so that the status of the IM and Presence Service database publisher nodes shows active.

Step 5 Repeat these steps for each VCS Control master node.

XCP Restart Notification from Cisco Telepresence Video Communication Server (VCS Control)

This information applies to CSCuo56821.

Following an upgrade of IM and Presence Service, VCS Control triggers an XCP restart notification which you can ignore.

Media Resources

Transcoder is Inserted for SIP Phones During a Midcall Codec Change

This information applies to CSCuo71657.

When a SIP endpoint is in an active call with call recording enabled and the far-end initiates a mid-call codec change, Unified Communications Manager now inserts a transcoder to maintain the integrity of the call. This enhancement allows you to use a mix of codecs (G.711 and G.729) in a distributed contact center with call recording. This functionality has been in place for SCCP endpoints since Release 8.5(1).

Miscellaneous

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.

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.

Devices Reset with Certificate Regeneration

This information applies to CSCus63274.

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

G.729 Millisecond Packet Size Limitation

This information applies to CSCut51778.

The **Preferred G.729 Millisecond Packet Size** service parameter applies to H323, MGCP, and SIP trunks. It does not apply to SIP-to-SIP IP Phone calls. SIP-to-SIP IP Phone calls use the default voice payload value of 20 ms.

Intermittent HTTP 500 Error with an SAML SSO Test

This information applies to CSCuj50309.

If you receive the following HTTP 500 error message while running an SAML SSO test, close the window and rerun the test:

```
IllegalArgumentException Invalid SAML request url
```

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.

Oauth Token Never Expires

This information applies to CSCuo80752.

To trigger OAuth timer expiration correctly, ensure that the OAuthTokenExpiry value on Unified Communications Manager is greater than the WebsessionApp expiry value on Tomcat.

Object ID in show hardware CLI Command Is Incorrect

This information applies to CSCun01808.

The object ID that is displayed after you run the **show hardware** command indicates only the system information in the Management Information Base (MIB). You cannot use the object ID to run the **utils snmp get** and **utils snmp walk** commands.

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.

RTP Library Components Update for 64 bit

The following is an update to the RTP Library Components. This information applies to CSCui40259.

Dynamic-Link Libraries

The following Dynamic-Link Libraries (DLLs) are installed as a part of the Cisco TAPI Service Provider (TSP) plugin and are used by the Cisco RTP Library:

Windows 32bit OS (x86):

- ciscortplib.dll
- ciscortpmon.dll
- ciscortpg711a.dll
- ciscortpg711u.dll
- ciscortpg729.dll
- ciscortppcm16.dll

Windows 64bit OS (x64):

- ciscortplib64.dll
- ciscortpmon64.dll
- ciscortpg711a64.dll
- ciscortpg711u64.dll

- ciscortpg72964.dll
- ciscortppcm1664.dll

RtpLib Callbacks Usage

This information applies to CSCuj63480.

An application can define a callback function in order to receive information about such things as operation completions, data transfers, and errors. Callback functions can be specified when an endpoint is created, when a stream callback is opened, and when a stream callback operation is initiated. If a callback operation is not specified, a corresponding stream callback is invoked if defined. If a stream callback is not specified, a corresponding callback endpoint is invoked if defined.

Note If you define the callback function, it is invoked for every operation that is initiated on a corresponding stream or endpoint. Consideration should be given to the case where a callback function is defined as a method in an object that is dynamically created and destroyed. In that case the destruction should not occur until all initiated operations are complete.

Endpoint Callback

Syntax

```
typedef void (WINAPI  *PRTPENDPOINTCALLBACK) (
  HANDLE           hEp,
  HANDLE           hStream,
  DWORD            dwError,
  PUCHAR           pData,
  DWORD            dwDataSize,
  LPVOID           pUserData,
  bool             bIsSilence,
  StreamDirection  streamDir
);
```

Parameters

hEp

Endpoint handle.

hStream

Rtp stream handle.

dwError

If not 0 (zero), indicates an error.

pData

Endpoint handle.

dwDataSize

Number of bytes received and transferred.

pUserData

Application data associated with an operation.

bIsSilence

If set to True, indicates that silence has been detected.

streamDir

Stream direction. Can be one of the following:

- ToApp
- ToNwk

Data Callback

Syntax

```
typedef void (WINAPI  *PRTPDATACALLBACK) (
  HANDLE           hStream,
  DWORD            dwError,
  PUCHAR           pData,
  DWORD            dwDataSize,
  LPVOID           pUserData,
  bool             bIsSilence
);
```

Parameters

hStream

Rtp stream handle.

dwError

If not 0 (zero), indicates an error.

pData

Endpoint handle.

dwDataSize

Number of bytes received and transferred.

pUserData

Application data associated with an operation.

bIsSilence

If set to True, indicates that silence has been detected.

Softkeys Not Working for 7936

This information applies to CSCut69616.

7936 phones use the Standard User as the default template. In order to use the conference, hold, transfer softkeys the Default template must be changed for Standard User. From **Device** > **Device Settings** > **Softkey Templates**, choose **Standard User** and check the **Default Softkey Template** option.

Speed Dial in Self Care Portal

This information applies to CSCun01472.

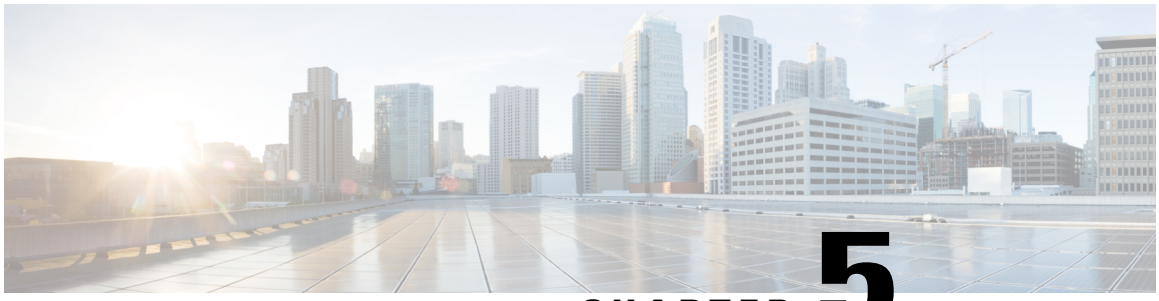
Speed-dial key assignments on the Self Care Portal are not the same as the speed-dial keys that you configure in the **Phone Configuration** window. We recommend that you see the "Speed-Dial and Abbreviated-Dial Setup" section in *Cisco Unified Communications Manager Administration Guide* before configuring speed dials in the Self Care Portal.

TFTP File Size Limit

This information addresses CSCuw28887.

You cannot upload files over 250 MB using TFTP file management in the OS Administration interface. If you try, the upload process times out.

To upload files above 250 MB, please work with the Cisco Technical Assistance Center (TAC).



CHAPTER 5

Caveats

- Bug Search Tool, page 49
- Resolved Caveats, page 50
- Open Caveats, page 50

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

Caveats

Open Caveats for Cisco Unified Communications Manager, Release 10.5(2)

Table 4: Open Caveats for Unified Communications Manager, Release 10.5(2)

Identifier	Severity	Component	Headline
CSCur55953	3	ccm-serviceability	Scheduled TraceCollection hangs indefinitely after SFTP down temporarily
CSCuo95791	3	cmui	CUCM Admin, axl, serviceability Vulnerable to CSRF Attack

Identifier	Severity	Component	Headline
CSCup27727	3	cmui	Client can control SQL data in CCMAdmin find list operations
CSCur79530	3	cpi-cert-mgmt	Self signed cert not deleted from Db when multi-service cert is uploaded
CSCuq77421	3	cpi-os	Increase size of common partition
CSCur59586	3	cpi-platform-api	not able to add CM instance in ELM/PLM when set accountlocking is enable
CSCur23720	3	cpi-security	Evaluation of SSLv3 POODLE vulnerability
CSCur30029	3	cp-mediacontrol	Ad-hoc Conference, B get reorder, in DOSIPTrunk-SME-DualStackV6Trunk
CSCur37231	3	cp-mediacontrol	Malformed or Missing Fast Start element in H225 CONNECT message
CSC uq94353	3	cp-mediacontrol	MOH resource(streams) are not released after the session is closed.
CSCup27824	3	cp-sip-trunk	SDL Signaling delay may cause intermittent Rendezvous Call failures
CSCun74317	3	cuc-tomcat	Potentially unsafe permissions on Tomcat directories
CSCuo95847	3	dna-ui	CUCM DNA Application Vulnerable to CSRF Attack
CSCuq02712	3	security	CUCM 10.5 Multi-Server CallManager cert disallows changing security mode

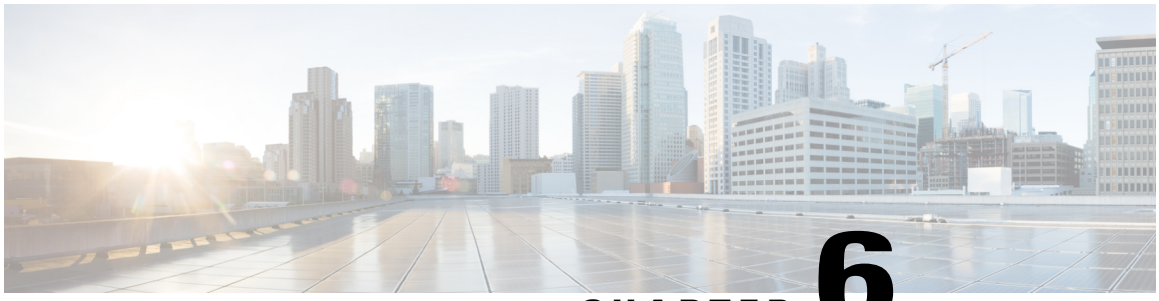
Open Caveats for IM and Presence Service, Release 10.5(2)

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

Identifier	Severity	Component	Headline
CSCus61289	3	cupxcpconfig	Cisco XCP Router service wont start due to bad internal configuration **Note** This Open Caveat applies to Release 10.5(2b).
CSCub71927	6	build_package	Script to automate commits to multiple branches
CSCua73880	3	ctigw	CUPS 8.6.4 is causing core dump with RCC
CSCur25679	2	cupxcpconfig	XCP Config Manager and XCP Services not Starting on IM&P
CSCup59213	3	database	Slow deleting of records in enduser table
CSCul10506	3	epe	Presence Engine produces a core dump when disabling calendaring for user
CSCuo04714	3	epe	HA: IMDB replication overwriting user presence after split brain recover
CSCur11673	3	gui	"User Must Change at Next Login" does not work correctly for IM/P webapp
CSCur78935	3	gui	Delay in CommonIPPMUtilities functions for retrieving node/subcluster

Identifier	Severity	Component	Headline
CSCur24611	3	gui	IM&P - External Database schema verification failed
CSCuq70164	2	gui-admin	AFT Troubleshooter - SSH to Ext File Server intermittently times out
CSCur06849	3	gui-admin	OutofBoundsException when special characters on CUP admin screens
CSCur41118	3	gui-localization	Localization issue can be seen under useflow Systems->Notifications
CSCuq62738	3	gui-serviceability	Serviceabillity UI not working with CA signed Tomcat Certs
CSCur66516	3	install	CUP goes to bad state since CUP upgraded while CUCM is being upgraded
CSCur87481	3	install	Sub IM&P 10.5.2 install doesn't continue using Touchless install feature
CSCuq83048	3	pws	Update PWS Developer Cookbook/Guide with latest PIDF examples
CSCur63497	3	security	IM&P server is vulnerable to user enumeration
CSCur85651	3	security	Certificate Exception seen in Serviceability due to Connection refusal
CSCur77947	3	serviceability	RTMT - XCP AFT logs filtering not happening w.r.t relative timings
CSCuo56545	3	sona	Config agent core on startup in the SONA library

Identifier	Severity	Component	Headline
CSCur36978	3	xcp-aft	File Transfer fails intermittently
CSCur38619	3	xcp-aft	Ext FS almost full - empty file gets uploaded but success is returned
CSCug38080	3	xcp-connmgr	CUP: Jabber CM Web Application Memory Exhaustion Vulnerability
CSCun59316	3	xcp-router	70% reduction in login throughput if IC peer is not contactable
CSCuo04591	3	xcp-router	MDNS recovery after network down taking too long
CSCur89511	3	xcp-router	IM&P system restart operation getting struck
CSCur92905	2	xcp-textconf	TC crashes when chat room destroyed with third-party compliance enabled



CHAPTER 6

Documentation Updates

- Administration Guide, page 56
- Bulk Administration Guide, page 67
- Call Detail Records Administration Guide, page 69
- CLI Reference Guide, page 73
- Disaster Recovery System Guide, page 74
- Features and Services Guide, page 75
- JTAPI Developers Guide, page 82
- Managed Services Guide, page 83
- Online Help for Cisco Unified Communications Manager, page 83
- OS Administration Guide, page 84
- Real-Time Monitoring Tool Guide, page 85
- Security Guide, page 86
- Serviceability Guide, page 91
- System Guide, page 94
- TAPI Developers Guide, page 97
- TCP and UDP Port Usage Guide, page 97
- Upgrade Guide, page 98
- Configuration and Administration Guide for IM and Presence Service, page 99
- Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service, page 99

Administration Guide

Cisco Unified IP Phone setup Description Character Length

This documentation update resolves CSCut08307.

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

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

Correction in IPv6 Address Field

This documentation update resolves CSCun07023.

The description for the **IPv6 Address (for dual IPv4/IPv6)** field in the *Cisco Unified Communications Manager Administration Guide* is incorrect. The following is the correct description.

Field	Description
IPv6 Address (for dualIPv4/IPv6)	This field supports IPv6. If your network uses DNS that can map to IPv6 addresses, you can enter the hostname of the Cisco Unified Communications Manager server. Otherwise, enter the non-link-local IP address of the Cisco Unified Communications Manager server; for information on how to obtain the non-link local IP address, see the *Cisco Unified Communications Manager Features and Services Guide*. This field, which is included in the TFTP configuration file, is used by phones that run SCCP and SIP to retrieve the IPv6 address of the Cisco Unified Communications Manager server. **Tip** Remember to update the DNS server with the appropriate Cisco Unified Communications Manager name and address information. **Tip** In addition to configuring the IPv6 Name field, you must configure the IP Address/Hostname field, so Cisco Unified Communications Manager can support features and devices that use IPv4 (or IPv4 and IPv6).

Correction in Software Conference Bridge Maximum Audio Streams

This documentation update resolves CSCuu44805.

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

Directory Number Field Description Updated

This documentation update resolves CSCur86259.

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

The Directory Number is a mandatory field.

Directory Number Line Behavior in Cisco Unified Communications Manager

This documentation update resolves CSCuo74599.

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

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

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

Disable Early Media on 180 Correction

This documentation update resolves CSCup68350.

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

Extension Mobility Now Supports Device Owners

This documentation update resolves CSCun04965.

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

Forbidden String When Configuring Directory Number Alert Names

This documentation update resolves CSCuv58163.

The following information is omitted from "Directory Number Settings" under topics related to Call Routing.

Caution Do not use the "Alert(" string anywhere in your Alerting Name or ASCII Alerting Name. Use of "Alert(" returns a security protocol error.

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

This documentation update resolves CSCur62680.

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

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

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

Hostnames in IPv4 and IPv6 Environments

This documentation update resolves CSCun74975.

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

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

Hub_None Location Correction

This documentation update resolves CSCuu40700.

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

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

ILS Data Sync to be Delayed Until after DB Replication is Completed

This documentation update resolves CSCuh55365.

The following note is omitted from the Directory number settings table in the *Cisco Unified Communications Manager Administration Guide* and from the Learned Global Dial Plan Data section in the *Cisco Unified Communications Manager Features and Services Guide*.

Note Cisco Unified Communications Manager pauses the recording of learned ILS patterns until replication of cluster is successfully established.

ILS Restictions for Directory URIs

This documentation update resolves CSCus74994.

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

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

Incorrect External Call Control Profile Field Description

This documentation update resolves CSCun07467.

The **External Call Control Profile** field is incorrectly described in the *Cisco Unified Communications Manager Administration Guide.* The following table contains the correct description.

Table 5: Directory Number Settings

Field	Description
Directory Number Information	
External Call Control Profile	In Cisco Unified Communications Manager, you enable external call control by assigning an external call control profile to a directory number. If the directory number has an external call control profile assigned to it, and when a call occurs that matches the directory number, Cisco Unified Communications Manager immediately sends a call-routing query to an adjunct route server, and the adjunct route server directs Cisco Unified Communications Manager on how to handle the call. For more information about external call control, see topics related to external call control in the *Cisco Unified Communications Manager Features and Services Guide*. From the drop-down list box, choose the external call profile that you want to assign to the directory number.

Incorrect Information about Deleting Route Patterns

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

The following information further explains the context:

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

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

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

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

The following is the corrected information:

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

Incorrect Note about User Locales

This documentation update resolves CSCuq42434.

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

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

Incorrect Time Period Example

This documentation update resolves CSCvb74432.

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

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

Insufficient Information about Call Control Agent Profile Fields

This documentation update resolves CSCuq11351.

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

The following table describes the Call Control Agent Profile settings.

Table 6: Call Control Agent Profile Settings

Field	Description
Call Control Agent Profile Configuration	
Call Control Agent Profile ID	Enter a unique ID for the Call Control Agent Profile. This ID is associated with the Directory Number. It is a mandatory field. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), and space ( ).
Primary Softswitch ID	Enter the primary softswitch ID (prefix) of the directory number alias servers. It is a mandatory field. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), and space ( ).
Secondary Softswitch ID	Enter the secondary softswitch ID (suffix) of the directory number alias servers. The allowed values for this field are alphanumeric (a-zA-Z0-9), period (.), dash (-), and space ( ).

Field	Description
Object Class	Enter the object class name for the directory numbers associated with the call control agent profile. It is a mandatory field. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), and space ( ).
Subscriber Type	Enter the subscriber type of the directory numbers associated with the call control agent profile. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), space ( ), and at (@).
SIP Alias Suffix	Enter the SIP alias suffix. The E.164 number that you specify for the directory number is appended to this suffix when mapping to the SIP Alias field in the LDAP directory. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), space ( ), and at (@).
SIP User Name Suffix	Enter the SIP user name suffix. The E.164 number that you specify for the directory number is appended to this suffix when mapping to the SIP User Name field in the LDAP directory. The allowed values are alphanumeric (a-zA-Z0-9), period (.), dash (-), space ( ), and at (@).

Line Group Deletion Correction

This documentation update resolves CSCuq26110.

The following is a correction to Line Group Deletion.

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

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

Location Menu Path

In the *Administration Guide*and online help, the Location field for H.225 and Intercluster Trunk Settings references the **System** > **Locations** menu. The correct menu path is **System** > **Location Info** > **Location**.

Maximum Hunt Timer Restriction

This documentation update resolves CSCuo90637.

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

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

Missing Information for Allow Multiple Codecs in Answer SDP

This documentation update resolves CSCup79162.

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

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

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

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

Phone Support for Multilevel Precedence and Preemption

This documentation update resolves CSCvb37715.

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

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

Remove Resource Priority Namespace List Field from SIP Profile Settings

This documentation update resolves CSCun32999.

The **Resource Priority Namespace List** field under **Device** > **Device Settings** > **SIP Profile** is listed in the *Cisco Unified Communications Manager Administration Guide* and online help, but has been removed from the **SIP Profile Configuration** window in Cisco Unified CM Administration.

Self-Provisioning Application Requires Phone Model with Security By Default

This documentation update resolves CSCun13382.

The following note is omitted from the "Self-Provisioning" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Note Phone models (such as Cisco IP Phone 7940 and 7960; IP Communicator series) that do not support the Security By Default (SBD) feature cannot use the Self-Provisioning service. This is because the self-provisioning feature that runs as an Idle URL supports HTTPS certificates only. These phones cannot verify the HTTPS certificates because they do not support the Trust Verification Service (TVS) functionality of the SBD feature.

However, these phones can still use the Self-Provisioning IVR service, provided that the phones themselves support the Self-Provisioning application.

Service Profiles and Device Owner User IDs

This documentation update resolves CSCuu43939.

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

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

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

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

SIP Trunk Fields SIP Trunk Status and SIPTrunk Duration

This documentation update resolves CSCun07961.

The following fields are omitted from "SIP Trunk Settings" in the *Cisco Unified Communications Manager Administration Guide*.

Field	Description
SIP Trunk status as determined by SIP OPTIONS Ping	
Full Service status (alarm—SIPTrunkISV) status	All the remote peers that are destinations of the SIP trunk are available. New call requests can be sent to any remote peer through the SIP trunk.
No Service status (alarm—SIPTrunk OOS)	All the remote peers that are destinations of the SIP trunk are unavailable. New call requests cannot be sent out via the SIP trunk.

Field	Description
Partial Service status (alarm—SIPTrunkPartiallyISV)	At least one remote peer is in service, but not all of the remote peers that are destinations of the SIP trunk are available. New call requests can be sent to an available remote peer through the SIP trunk.
Unknown—OPTIONS Ping not enabled	The SIP trunk status is unknown when SIP OPTIONS Ping is not enabled.

Synchronize Trunks and Gatekeeper Sections Are Not Valid

This documentation update resolves CSCuq05944.

The following changes are applicable because the **Apply Config to Selected** button is not available in **Cisco Unified CM Administration** :

- "Synchronize Trunk" section is removed from the "Trunk Setup" chapter
- "Synchronize Gatekeeper" section is removed from the "Gatekeeper Setup" chapter

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.

Insufficient Information About Automatic Fallback

This documentation update resolves CSCuz01075. The **Deployment models** chapter in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* contains insufficient information about the Automatic Fallback field. The following has been omitted from the guide.

Automatic FallbackIM and Presence Service supports automatic fallback to the primary node after a failover. Automatic fallback is the process of moving users back to the primary node after a failover without manual intervention. You can enable automatic fallback with the Enable Automatic Fallback service parameter on the Cisco Unified CM IM and Presence Administration interface. Automatic fallback occurs in the following scenarios:

- A critical service on Node A fails—A critical service (for example, the Presence Engine) fails on Node A. Automatic failover occurs and all users are moved to Node B. Node A is in a state called “Failed Over with Critical Services Not Running”. When the critical service recovers, the node state changes to "Failed Over." When this occurs Node B tracks the health of Node A for 30 minutes. If no heartbeat is missed in this timeframe and the state of each node remains unchanged, automatic fallback occurs.
- Node A is rebooted—Automatic failover occurs and all users are moved to Node B. When Node A returns to a healthy state and remains in that state for 30 minutes automatic fallback will occur.
- Node A loses communications with Node B—Automatic failover occurs and all users are moved to Node B. When communications are re-established and remain unchanged for 30 minutes automatic fallback will occur.

If failover occurs for a reason other than one of the three scenarios listed here, you must recover the node manually. If you do not want to wait 30 minutes before the automatic fallback, you can perform a manual fallback to the primary node. For example: Using presence redundancy groups, Cisco Jabber clients will fail over to a backup IM and Presence Service node if the services or hardware fail on the local IM and Presence Service node. When the failed node comes online again, the clients automatically reconnect to the local IM and Presence Service node. When the failed node comes online, a manual fallback operation is required unless the automatic fallback option is set. You can manually initiate a node failover, fallback, and recovery of IM and Presence Service nodes in the presence redundancy group. A manual fallback operation is required unless the automatic fallback option is set.

UDS in Remote Cluster Service Configuration is Not Supported

This documentation update resolves CSCuv67224.

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

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.

LDAP Authentication Correction

This documentation update resolves CSCux00028.

The “Update LDAP Authentication ” section in the *Cisco Unified Communication Manager Administration Guide* contains incorrect information about “LDAP Authentication”. The description states that the LDAP

synchronization must be disabled to make changes to the LDAP authentication settings. The correct information for "LDAP Authentication" is as follows:

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

Authenticate with Multiple LDAP Domains

This documentation update resolves CSCuy37309.

Note When you are using the sAMAccountName value for the **LDAP Attribute for User ID** field, you can only authenticate with one LDAP Domain. To authenticate with multiple domains, you need to use the Active Directory Lightweight Directory Service (AD LDS).

Field	Description
LDAP User Search Base	Enter the location (up to 256 characters) where all LDAP users exist. This location acts as a container or a directory. This information varies depending on customer setup. **Note** This field is mandatory.

Certificate Monitor Frequency Interval

This documentation update resolves CSCvc32210.

The following note is omitted from the "Monitor Certificate Expiration" procedure in the *Administration Guide for Cisco Unified Communications Manager*.

Note The certificate monitor service runs every 12 hours by default. When you restart the certificate monitor service, it starts the service and then calculates the next schedule to run only after 12 hours. The interval does not change even when the certificate is close to the expiry date of seven days. It runs every 1 hour when the certificate either has expired or is going to expire in one day.

Bulk Administration Guide

Bulk Administration Character Length

This documentation update resolves CSCum94975.

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

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

Bulk Administration Gateway Deletion Changes

This documentation update resolves CSCup31813.

The “Delete Cisco Gateway Records Using Query” topic in the *Bulk Administration Guide* contains only a partial list of gateways that you can delete by using query. The following paragraph is the correct information:

You can use a query to locate the gateway records that you want to delete from Cisco Unified Communications Manager. You can only delete Cisco VG200, VG202, VG204, VG224, VG350 and Cisco Catalyst 6000 gateways using the Delete Gateway Configuration window.

EMCC Device Calculation in the Bulk Administration Tool

This documentation update resolves CSCuy38765.

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

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

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

Removed Fields in Delete User Device Profiles Custom Configuration

This documentation update resolves CSCup36738.

The following changes are applicable for “Delete User Device Profiles Custom Configuration.”

- **Directory Number** field is removed
- Custom is removed from the window title **Delete User Device Profiles Custom Configuration**
- Removed the step: In the Delete drop-down list box choose one of the following options:
  - User
  - Autogenerated
  - All

TAPS and Cisco UCCX with a Standard License

This documentation update resolves CSCus36476.

The following note is omitted from the "Tool for Auto-Registered Phones Support (TAPS)" chapter in the *Bulk Administration Guide*.

Note The TAPS application does not work with a Cisco UCCX Standard license. You must use either an Enhanced or Premium license.

Call Detail Records Administration Guide

Four New Fields in Call Details Record

This documentation update resolves CSCun19226.

The following table describes the new fields that are omitted from the *Call Details Record Administration Guide*.

Field Name	Range of Values	Description
originalCalledPartyPattern	Text String	Numeric string (with special characters) up to 50 characters. This is the pattern to which the original call was placed before any configured translation rules are applied. Default—empty string "".

Field Name	Range of Values	Description
finalCalledPartyPattern	Text String	Numeric string (with special characters) string up to 50 characters. The pattern of the final called party to which the call is presented until that call is answered or ringing has ended. If no forwarding occurred, this pattern is the same as originalCalledPartyPattern. This field indicates the pattern before any configured translation rules are applied. This value is the same as the finalCalledPartyNumber if the number is a direct match without any translation Default—empty string "".
lastRedirectingPartyPattern	Text String	Numeric string (with special characters) string up to 50 characters. The pattern of the last party which redirected the call to the current called party. If there is no redirection, the field has the same value as the originalCalledPartyPattern. Default—empty string "".
huntPilotPattern	Text String	Numeric string (with special characters) string up to 50 characters. The huntPilot pattern as configured in the database. This field is populated only when the HuntPilot member answers the call which is placed either directly or as a result of redirection to the huntPilot. Default - empty string "". If no huntPilot member answers, this field will be empty.

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

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

FieldNames	Orig Call CDR	Setup Call CDR	Conference CDR 1	Conference CDR 2	Conference CDR 3	Final CDR
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.

Support Removed for utils vmtools status

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

Disaster Recovery System Guide

Supported SFTP Servers

This documentation update resolves CSCur96680.

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

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

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

Table 7: SFTP Server Information

SFTP Server	Information
SFTP Server on Cisco Prime Collaboration Deployment	This server is provided and tested by Cisco, and supported by Cisco TAC. Version compatibility depends on your version of Unified Communications Manager and Cisco Prime Collaboration Deployment. See the *Cisco Prime Collaboration Deployment Admin Guide* before you upgrade its version (SFTP) or Unified Communications Manager to ensure that the versions are compatible.

SFTP Server	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.

Features and Services Guide

Add or Update Hosted DN Pattern Through CSV File

Procedure

Follow one of these procedures, depending on your configuration:

- If the Hosted DN Group is selected by a Call Control Discovery (CCD) Advertising Service:
  1. Create a new Hosted DN Group to perform the upload.
  2. Delete the CCD Advertising Service.
  3. Upload the existing Hosted DN Group.
  4. Recreate the CCD Advertising Service.

  The CCD Advertising Service unpublishes all existing patterns and republishes newly added patterns.
- If the Hosted DN Group is not selected by a CCD Advertising Service, upload a CSV file directly to replace all Hosted DN Patterns.

Call Pickup Group Visual Notification Does Not Support Localization

This documentation bug resolves CSCup04321.

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

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.

Cisco Unified Communications Manager Sends INVITE Message to VCS

This documentation update resolves CSCuv22205.

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

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

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

This documentation update resolves CSCva32400.

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

Cisco Jabber does not support CMCs or FACs.

Client Matter Codes, Forced Authorization Codes, and Failover Calls

This documentation update resolves CSCuv41976.

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

CMCs and FACs do not support failover calls.

Corrected License Report Update Interval

This documentation update resolves CSCuv84693.

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

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

Corrections for the Immediate Divert Feature

This documentation update resolves CSCun20448.

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

Configure Immediate Divert

Step 6

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

Step 7

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

System requirements for Immediate Divert

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

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

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

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

Cisco Unified Mobility Documentation Changes

This documentation update resolves CSCun14245.

Replace references to *Cisco Unified Mobile Communicator* with *dual-mode phones*.

For example, "a Cisco Unified Mobile Communicator-enabled dual-mode mobile identity" should read "a dual-mode phone mobile identity."

The following parameters are omitted from the Remote Destination Configuration fields:

- **Owner User ID—**From the drop-down list, choose the user ID of the assigned Remote Destination user. The user ID is recorded in the call detail record (CDR) for all calls made from this device.
- **Enable Unified Mobility Features—**Check this check box to enable Unified Mobility features for this remote destination.
- **Enable Extend and Connect—**Check this check box to allow this phone to be controlled by CTI applications (for example, Jabber). For more information, see the *Features and Services Guide for Cisco Unified Communications Manager*.

Replace the parameter field **Mobile Phone** with **Enable Move to Mobile**. Replace the parameter field **Enable Cisco Unified Mobility** with **Enable Single Number Reach**.

Default Partitions

This documentation update resolves CSCum99459.

The following partitions are Cisco-provided default partitions:

- Directory URI
- Global Learned E.164 Numbers
- Global Learned E.164 Patterns
- Global Learned Enterprise Numbers
- Global Learned Enterprise Patterns

For information about Global Learned E.164 Numbers, Global Learned E.164 Patterns, Global Learned Enterprise Numbers, and Global Learned Enterprise Patterns, see the "Partitions for Learned Patterns Settings" section in the *Features and Services Guide for Cisco Unified Communications Manager*.

Directory URI

The Directory URI is a system partition, introduced in Cisco Unified Communications Manager Release 9.0(1), which Cisco Unified Communications Manager automatically creates based on the Directory URIs that are provisioned in the **End User Configuration** window and an association between end users and DNs through a primary extension. You can edit the Directory URI partition but cannot delete it.

For more information about Directory URIs, see the "URI Dialing" chapter in the *Features and Services Guide for Cisco Unified Communications Manager*.

Incorrect Multicast Music On Hold Restriction

This documentation update resolves CSCvb28136.

In the Music On Hold (MOH) configuration chapter, a restriction incorrectly states that you should configure unicast MOH to avoid silence on the line when an MTP resources is invoked. The correct restriction is as follows:

When an MTP resource gets invoked in a call leg at a site that is using multicast MOH, Cisco Unified Communications Manager falls back to unicast MOH instead of multicast MOH.

Force Authorization Codes Not Supported on Cisco Jabber

This documentation update resolves CSCuz63406.

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

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

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.

Locations Media Resource Audio Bit Rate Policy Service Parameter Limitation

This documentation update resolves CSCux90107.

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

The Locations Media Resource Audio Bit Rate Policy service parameter does not have any impact if there is no media in one of the call legs. In such cases, location bandwidth manager deducts the maximum hop bandwidth that is configured for the source destination from the available bandwidth of that location.

Music On Hold and Native Call Queuing Behavior

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

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

Remote Destination and Auto Answer

This documentation update resolves CSCtd43582.

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

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

Restart Intercluster Lookup Service

This documentation update resolves CSCuv11445.

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

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

SAF Forwarder and Requesting Service Arrow Keys Removed

This documentation update resolves CSCun02017.

The "SAF Forwarder Configuration" and "CCD Requesting Service Configuration" topics in the *Features and Services Guide for Cisco Unified Communications Manager* state that you can order items in a pane by highlighting them and clicking the up and down arrows to the right of the pane. This function was removed from the administrative interface.

SAML Not Enabled after Upgrade on Web Dialer

This documentation update resolves CSCun17524.

The following procedure is omitted from “Enable SAML SSO” section in the *Cisco Unified Communications Manager Features and Services Guide*.

Follow this procedure to enable SAML Single Sign-On (SSO) on Cisco Web Dialer after an upgrade.

Procedure

Step 1 Deactivate the Cisco Web Dialer web service if it is already activated.

Step 2 Disable SAML SSO if it is already enabled.

Step 3 Activate the Cisco Web Dialer web service.

Step 4 Enable SAML SSO.

SAML SSO Authentication LDAP Attribute for User ID Setting

This documentation update resolves CSCuq44567.

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

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

Video Capabilities and Enhanced Location Call Admission Control

This documentation update resolves CSCut20187.

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

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

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.

JTAPI Developers Guide

MeetMe: Unsupported JTAPI Feature

This documentation update resolves CSCum39340.

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

Unsupported CTI Events From SIP Phones

This information resolves CSCur36240.

The *Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager* and the *Cisco Unified TAPI Developers Guides for Cisco Unified Communications Manager* do not provide details on the following CTI events. These CTI events are not supported for SIP phones. Developers who are programming third party applications that invoke these CTI events should use SCCP phones.

- CallOpenLogicalChannelEvent
- CallRingEvent
- DeviceLampModeChangedEvent
- DeviceModeChangedEvent
- DeviceDisplayChangedEvent
- DeviceFeatureButtonPressedEvent
- DeviceKeyPressedEvent
- DeviceLampModeChangedEvent
- DeviceRingModeChangedEvent

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.

Online Help for Cisco Unified Communications Manager

Backup Device Limit Incorrect in Disaster Recovery System Online Help

This documentation update resolves CSCuu94393.

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

Incorrect Description for Destination Number

This documentation update resolves CSCux74230.

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

Directory Number Field Description Updated

This documentation update resolves CSCuy28500.

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

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

Remote Destination Configuration Page In the OLH Needs To Be Updated

This documentation update resolves CSCvb88447.

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

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

OS Administration Guide

Documentation Update for Certificate Monitor Configuration

This documentation update resolves CSCuo30610.

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

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

Add CA Signed CAPF Root Certificate to Trust Store

This documentation update resolves CSCut87382.

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

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

Procedure

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

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

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

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

Real-Time Monitoring Tool Guide

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

This documentation update resolves CSCuq28511.

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

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

Incorrect Default Value for LogPartitionLowWaterMarkExceeded Alert

This documentation update resolves CSCuq39087.

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

Table 9: Default Configuration for the LogPartitionLowWaterMarkExceeded RTMT Alert

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

Incorrect Minimum Rate for Monitoring a Performance Counter

This documentation update resolves CSCuz11160.

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

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

New LowAvailableVirtualMemory Threshold

This documentation update resolves CSCuu72197.

The LowAvailableVirtualMemory threshold in the *Cisco Unified Real-Time Monitoring Tool Administration Guide* is listed as below 30%. For Release 10.5(2), the new threshold value is below 15%.

FQDN Support to Display Hostnames in RTMT

This documentation update resolves CSCun02558.

To use the Trace and Log Central feature, make sure that the Cisco Unified Real-Time Monitoring Tool can directly access the node or all of the nodes in a cluster without Network Address Translation (NAT). If you configured a NAT to access devices, configure the nodes with a hostname instead of an IP address and make sure that the hostnames (Fully Qualified Domain Name of the host) and their routable IP address are in the DNS node or host file.

RTMT Mail Server Procedure Correction

This documentation update resolves CSCun08876.

The "Add or Edit Mail Server" procedure contains an incorrect step: "In the **Sender UserID** field, enter the sender user ID that you need to notify." The Cisco Unified Real-Time Monitoring Tool does not have a Sender UserID field; disregard this step.

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.

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.

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
```

Enable Password Persistence

This documentation update resolves CSCuy05368.

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

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

Default: False

Resync Bandwidth Option is Removed

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

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

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

This documentation update resolves CSCuz68165.

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

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

ITL File Size Limitation

This documentation update resolves CSCvb44649.

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

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

Serviceability Guide

Cisco CAR DB Service

This documentation update resolves CSCup98304.

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

Cisco CAR DB Service

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

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

Cisco Certificate Change Notification Service

This documentation update resolves CSCup84785.

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

Cisco Certificate Change Notification Service

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

Cisco IP Phone Service Removed from CM Services

This documentation update resolves CSCur03499.

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

Cisco SOAP-CallRecord Service

This documentation update resolves CSCup98302.

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

Cisco SOAP-CallRecord Service

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

Delayed Initialization after IP Manager Assistant Service Restart

This documentation update resolves CSCus78713.

The following information is omitted from the "CTI Services" chapter in the *Serviceability Administration Guide*:

Expect a 12 to 15 minute delay after you restart the Cisco IP Manager Assistant service with a full resource load of 7000 users and 7000 phones.

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.

Self Provisioning IVR Service

This documentation update resolves CSCum57057.

Although it appears in the *Cisco Unified Serviceability Administration Guide* and online help, the Self Provisioning IVR Service is unavailable in the **Alarm Configuration** window in Cisco Unified Serviceability.

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>**.

Minimize Disk Space utilized by Log Files

This documentation update resolves CSCva35260.

The following entry is omitted from the “Audit Log Configuration Settings” table in the *Cisco Unified Serviceability Administration Guide*.

Field	Description
Set to Default	The **Set to Default** button specifies the default values. It is recommended to set the audit logs to default mode unless it is required to be set to a different level for detailed troubleshooting. The **Set to Default** option minimizes the disk space utilized by log files.

System Guide

Call Transfer to Hunt Pilot Restriction

This documentation update resolves CSCuw57732.

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

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

Email IDs on the Active Directory Server

This documentation update resolves CSCur55902.

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

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

LDAP Directory Support

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

The complete list of supported directories is as follows:

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

Bandwidth Calculations

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

Insufficient Information About Adding a New ILS Hub

This documentation update resolves CSCva25662.

The following restriction is omitted from the " Configure Intercluster Lookup Service" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*:

Restriction	Description

ILS Hub	When adding an additional hub cluster into the ILS network ensure to verify the following conditions are met for the primary ILS hub node: • Cluster ID is unique across all the hub nodes in the ILS cluster. • Fully Qualified Domain Name (FQDN) is configured. • UDS and EM services are running on the all of the hub nodes in the ILS cluster. • DNS primary and reverse resolution are working fine. • Import consolidated Tomcat certificates from all the hub nodes. Else, the "version" information will not get displayed in the **Find and List Remote Clusters** window even after rebooting the clusters or correcting the errors. The workaround is to remove the hub cluster from the ILS network, comply with the above requirements and add the hub cluster back into the ILS network.

Insufficient Information About Third-Party Restrictions

This documentation update resolves CSCvc16660.

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

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

Time of Day routing not Implemented for Message Waiting Indicator

This documentation update resolves CSCva13963.

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

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

TAPI Developers Guide

Unsupported CTI Events from SIP Phones

This information resolves CSCur36240.

The *Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager* and the *Cisco Unified TAPI Developers Guides for Cisco Unified Communications Manager* do not provide details on the following CTI events. These CTI events are not supported for SIP phones. Developers who are programming third party applications that invoke these CTI events should use SCCP phones.

- CallOpenLogicalChannelEvent
- CallRingEvent
- DeviceLampModeChangedEvent
- DeviceModeChangedEvent
- DeviceDisplayChangedEvent
- DeviceFeatureButtonPressedEvent
- DeviceKeyPressedEvent
- DeviceLampModeChangedEvent
- DeviceRingModeChangedEvent

TCP and UDP Port Usage Guide

Missing Information about TCP Port 22

This documentation update resolves CSCus05634.

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

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

Missing Information about TCP Port 5555

This documentation update resolves CSCus26925.

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

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

Missing Information about Common Service Port 8006

This documentation update resolves CSCuy48628.

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

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

Upgrade Guide

Disable or Postpone LDAP Synchronization During an Upgrade

This document update resolves CSCuq07331.

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

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

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

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

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

Unified CM 10.0 Upgrade Process Correction

This documentation update resolves CSCup31306.

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

Configuration and Administration Guide for IM and Presence Service

UDS Directory Supported with Directory URI IM Addressing

This documentation update resolves CSCuu34045.

The *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* states that a directory URI IM addressing scheme does not support UDS-based directory integration. However, this information is incorrect. A directory URI IM addressing scheme does support UDS based directory integration.

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.

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*.