# Release Notes for Cisco Unified Communications Manager and IM and Presence Service, Release 10.5(1)

**First Published:** 2014-05-07

**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-32173-01

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

© 2016 Cisco Systems, Inc. All rights reserved.

# CONTENTS


CHAPTER 1 **Introduction** 1

About Release Notes 1

Documentation for Release 10.5(1) 2

Upgrades 2

Supported Web Browsers 2

Cisco Unified Communications Manager Administration 2

Cisco Unified Analysis and Reporting and Cisco Unified Serviceability 2

Self Care Portal 3

CHAPTER 2 **Upgrades** 5

Software Versions 5

Supported Upgrades 5

Important Notes about Upgrades 6

No Configuration During Upgrades 6

Preupgrade COP File 6

Upgrades from IM and Presence Service 10.0(1) Export Unrestricted 7

Upgrade Fails if AXL Password Contains Special Characters 8

OS Administrator Account Required for IM and Presence Upgrades 8

CHAPTER 3 **New and Changed Features** 9

New Default Softkey Templates for Feature Hardkey Phones 10

Cluster-wide Multiserver Certificate Support 10

Multiserver Certificate Overview 11

Multiserver Certificate Benefits 12

Manage Certificates 16

Configure Multiserver Certificate 17

Generate Certificate Signing Request for Multiserver Certificate 18

Download Certificate Signing Request for Single-Server and Multiserver Certificate 19
SAML Single Sign-On 19
JTAPI Support for Single Sign-On 21
Acquire the Single Sign-On Token 22
Interface Changes for Single Sign-On Oauth Support 24
Use Cases for Single Sign-On Oauth Support 24
TAPI Support for Single Sign-On 27
TAPI Use Cases for Single Sign-On Support 29
Web Dialer Single Sign-On Support 31
SIP Best Effort Early Offer 31
SIP Best Effort Early Offer Benefits 32
Set Up SIP Trunk 33
SIP Profile Settings 33
Daylight Saving Time Rules 36
DST-CiscoSyslog Messages 36
utils update dst 38
Directory Search in Self Care 39
Embedded Cisco TelePresence Management Suite in Self Care Portal 39
Enable Embedded TelePresence for Self Care Portal 39
IM and Presence Service Deprecation of Microsoft Exchange Server 2003 40
IM and Presence Service Deprecation of WebDAV 40
IM and Presence Service IPv6 Support 40
IPv6 Configuration 40
IPv6 Interactions and Restrictions 41
New CLI Commands 42
set network ipv6 dhcp 42
set network ipv6 gateway 42
set network ipv6 service 43
set network ipv6 static_address 44
IM and Presence Service Support for Encrypted External Database 44
Support Variable Extension Length and +E.164 for LDAP Directory Numbers 45
Voice Gateway Support 47
Cisco Voice Gateways (ISR) 44XX Series 47
Cisco ISR44XX Series Gateways 48

Cisco Integrated Services Router 4451-X 48
Cisco Voice Gateways 48
Standalone Voice Gateways 50
Cisco VG310 Analog Phone Gateway 50
Cisco VG320 Analog Phone Gateway 50
Cisco VG350 Analog Phone Gateway 50
Voice Gateway Model Summary 50
New CLI Commands 51
utils vmtools refresh 51
Windows 8.1 and Windows Server 2012 R2 Support 52
About Cross-Origin Resource Sharing 52
Configure Cross-Origin Resource Sharing 53
Configure LDAP Directory 53
New RTMT Alert for Global Dial Plan Replication 54
Silent Monitoring CLI Update 55
Set replication-sync monitor 55
Product-Specific Configuration in TelePresence Device User Interfaces 55
Cisco IP Phones and Cisco Desktop Collaboration Experience DX650 56
Cisco IP Phones 56
Cisco IP Phone Firmware Versions 56
Cisco Unified SIP Phone 3905 Features 56
Cisco Unified IP Phone 6900 Series Features 56
Cisco IP Phone 7800 Series Features 57
Cisco Unified IP Phone 7900 Series Features 57
Cisco Unified Wireless IP Phone 792x Series Features 57
Cisco Unified IP Conference Phone 8831 Features 57
Cisco Unified IP Phones 8941 and 8945 Features 58
Cisco Unified IP Phones 8961, 9951, and 9971 Features 59
Cisco DX Series 59
Cisco DX650 Firmware Versions 59
Cisco DX650 Features 59

CHAPTER 4 **Important Notes** 61
Call Control 61
Conference Call Video Problem 61

SIP IPv6 Calls Fail When Using UDP 62
Installation 62
Floppy Image Needed for Unattended Installations 62
Installation Warnings 62
Disaster Recovery System 62
DRS Restore of Failed IM and Presence Service Database Publisher Node Requires DRS Restore of Cisco Unified Communications Manager Publisher Node 62
DRS Restore Status Shows Failed Due to a DB Restore Failure Condition 63
Features and Services 63
6900 Series Phones Fail to Connect When Accessing Personal or Corporate Directories 63
USB Music on Hold Fixed Audio Adapter is not Supported 63
IM and Presence Service 64
Availability and IM Broken Between Publisher and Subscriber After Upgrade 64
Enable or Disable FIPS for IM and Presence Service 64
IM and Presence Service Needs to Support Install Against a Small Disk Cisco Unified Communications Manager Publisher 64
Interoperability 65
Cisco Unified Mobility Disclaimer 65
Failure to Add Unified CM Cluster for Collaboration Edge with TLS Verify Enabled If Unified CM Shares Certificate 65
Failover Interoperability with Cisco Jabber Clients 65
XCP Restart Notification from Cisco Telepresence Video Communication Server (VCS Control) 66
Miscellaneous 66
Cisco Unified IP Phones 7940 and 7960 Do Not Support Java Midlets 66
Intermittent HTTP 500 Error with an SAML SSO Test 66
Oauth Token Never Expires 66
Object ID in show hardware CLI Command Is Incorrect 66
Presence Web Service Unable to Send Event Notification if Endpoint Registered with FQDN 66
RTP Library Components Update for 64 bit 67
RtpLib Callbacks Usage 67
Speed Dial in Self Care Portal 69
SIP Trunk Not Properly Reset until CFB is Reset 69
Devices Reset with Certificate Regeneration 70

MGCP IOS Gateway From PSTN Does Not Support Connected Address in ISDN Notify 70
Perfect Forward Secrecy is not Supported in IPsec Configuration 70
Change Perfmon Counter File Size Parameters in RTMT 70

CHAPTER 5 Documentation Updates 71
Administration Guide 72
Cisco Unified IP Phone setup Description Character Length 72
Correction in IPv6 Address Field 72
Correction in Software Conference Bridge Maximum Audio Streams 73
Directory Number Field Description Updated 73
Directory Number Line Behavior in Cisco Unified Communications Manager 73
Disable Early Media on 180 Correction 74
Extension Mobility Now Supports Device Owners 74
Forbidden String When Configuring Directory Number Alert Names 74
Hostname and IP Address Field Can Contain a Fully Qualified Domain Name 74
Hostnames in IPv4 and IPv6 Environments 75
Hub_None Location Correction 75
ILS Data Sync to be Delayed Until after DB Replication is Completed 75
ILS Restictions for Directory URIs 75
Incorrect External Call Control Profile Field Description 75
Incorrect Information about Deleting Route Patterns 76
Incorrect Note about User Locales 77
Incorrect Time Period Example 77
Insufficient Information about Call Control Agent Profile Fields 77
Line Group Deletion Correction 78
Location Menu Path 78
Maximum Hunt Timer Restriction 78
Missing Information for Allow Multiple Codecs in Answer SDP 79
Phone Support for Multilevel Precedence and Preemption 79
Remove Resource Priority Namespace List Field from SIP Profile Settings 79
Self-Provisioning Application Requires Phone Model with Security By Default 79
Service Profiles and Device Owner User IDs 80
SIP Trunk Fields SIP Trunk Status and SIPTrunk Duration 80
Synchronize Trunks and Gatekeeper Sections Are Not Valid 81
Transmit UTF8 for Calling Party Name Field Correction 81

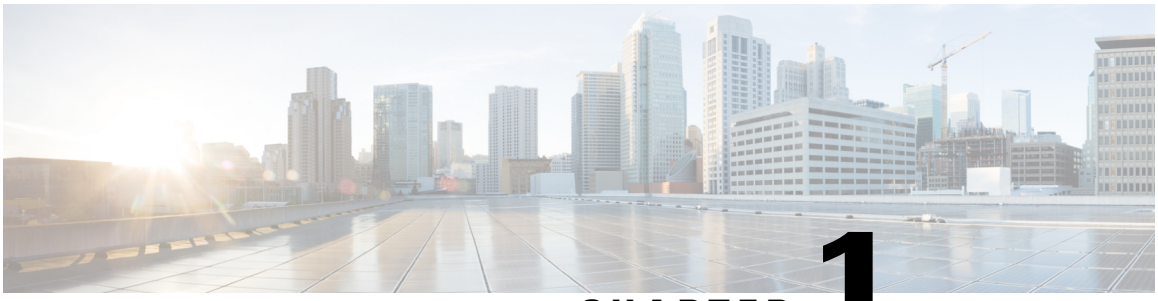
Insufficient Information About Automatic Fallback 81
UDS in Remote Cluster Service Configuration is Not Supported 82
A Server Restart is Required After Uploading a Certificate 82
LDAP Authentication Correction 82
Authenticate with Multiple LDAP Domains 83
Bulk Administration Guide 83
Bulk Administration Character Length 83
Bulk Administration Gateway Deletion Changes 83
EMCC Device Calculation in the Bulk Administration Tool 84
Removed Fields in Delete User Device Profiles Custom Configuration 84
TAPS and Cisco UCCX with a Standard License 84
Call Detail Records Administration Guide 85
Four New Fields in Call Details Record 85
FAC and CMC Code is not Captured in CDR 86
CLI Reference Guide 89
ILS Troubleshooting Tips Corrections 89
Show perf query counter Command Output 89
Support Removed for utils vmtools status 89
Disaster Recovery System Guide 89
Supported SFTP Servers 89
Features and Services Guide 90
Add or Update Hosted DN Pattern Through CSV File 90
Call Pickup Group Visual Notification Does Not Support Localization 91
Calling Party Normalization Restriction 91
Cisco Unified Communications Manager Sends INVITE Message to VCS 91
Client Matter Codes and Force Authorization Codes Not Supported on Cisco Jabber 92
Client Matter Codes, Forced Authorization Codes, and Failover Calls 92
Corrected License Report Update Interval 92
Corrections for the Immediate Divert Feature 92
Cisco Unified Mobility Documentation Changes 93
Default Partitions 94
Incorrect Multicast Music On Hold Restriction 94
Force Authorization Codes Not Supported on Cisco Jabber 94
Incorrect Report for Device Mobility 94
Jabber Devices Count as Registered Devices 95

Locations Media Resource Audio Bit Rate Policy Service Parameter Limitation 95
Music On Hold and Native Call Queuing Behavior 95
Remote Destination and Auto Answer 95
Restart Intercluster Lookup Service 95
SAF Forwarder and Requesting Service Arrow Keys Removed 96
SAML Not Enabled after Upgrade on Web Dialer 96
SAML SSO Authentication LDAP Attribute for User ID Setting 96
Video Capabilities and Enhanced Location Call Admission Control 96
Call Pickup Restriction 97
JTAPI Developers Guide 97
MeetMe: Unsupported JTAPI Feature 97
Unsupported CTI Events From SIP Phones 97
Managed Services Guide 98
SNMP Limits 98
Online Help for Cisco Unified Communications Manager 98
Backup Device Limit Incorrect in Disaster Recovery System Online Help 98
Incorrect Description for Destination Number 98
Directory Number Field Description Updated 98
Remote Destination Configuration Page In the OLH Needs To Be Updated 99
OS Administration Guide 99
Documentation Update for Certificate Monitor Configuration 99
Add CA Signed CAPF Root Certificate to Trust Store 99
Real-Time Monitoring Tool Guide 100
Analyze Call Path Tool does not Work with Non-English Language 100
Incorrect Default Value for LogPartitionLowWaterMarkExceeded Alert 100
Incorrect Minimum Rate for Monitoring a Performance Counter 100
LowAvailableVirtualMemory Threshold Value is Incorrect 101
FQDN Support to Display Hostnames in RTMT 101
RTMT Mail Server Procedure Correction 101
Security Guide 101
Bulk Certificate Import May Cause Phones To Restart 101
Replace ASA Certificate on AnyConnect VPN Phone 102
Secure and Nonsecure Indication Tone 102
Incorrect Configuration Example for ASA Router 103
Enable Password Persistence 105

Resync Bandwidth Option is Removed 105
CNF File Encryption Is Not Supported by Default on 6901 and 6911, Cisco IP Phones 105
ITL File Size Limitation 106
Serviceability Guide 106
Cisco CAR DB Service 106
Cisco Certificate Change Notification Service 106
Cisco IP Phone Service Removed from CM Services 107
Cisco SOAP-CallRecord Service 107
Delayed Initialization after IP Manager Assistant Service Restart 107
Platform Administrative Web Service 107
Self Provisioning IVR Service 108
SNMP Limits 108
IM and Presence Security Best Practice 108
SOAP-Diagnostic Portal Database Service 108
Error in SYSLOG-MIB Parameters 109
Minimize Disk Space utilized by Log Files 109
System Guide 109
Call Transfer to Hunt Pilot Restriction 109
Email IDs on the Active Directory Server 109
LDAP Directory Support 110
Bandwidth Calculations 110
Insufficient Information About Adding a New ILS Hub 110
Insufficient Information About Third-Party Restrictions 111
Time of Day routing not Implemented for Message Waiting Indicator 111
TAPI Developers Guide 112
Unsupported CTI Events from SIP Phones 112
TCP and UDP Port Usage Guide 112
Missing Information about TCP Port 22 112
Missing Information about TCP Port 5555 112
Missing Information about Common Service Port 8006 113
Upgrade Guide 113
Disable or Postpone LDAP Synchronization During an Upgrade 113
InterCluster Peer-User and Admin-CUMA Application User Roles Deprecated 113
Unified CM 10.0 Upgrade Process Correction 114
Configuration and Administration Guide for IM and Presence Service 114

Retrieve Chat Rooms on a Replaced Node 114
Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service 114
Domain Name Change for Cisco Unified Communications Manager 114
Update Domain Name for Cisco Unified Communications Manager 114

CHAPTER 6 Caveats 117
Bug Fixes and Updates 117
Bug Search Tool 117
Resolved Caveats 118
Open Caveats 118
Caveats 118
a-Open Caveats for Cisco Unified Communications Manager, Release 10.5(1) 118
Open Caveats for IM and Presence Service, Release 10.5(1) 121



CHAPTER 1

# Introduction


- About Release Notes, page 1
- Documentation for Release 10.5(1), 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 for collaborative communication.

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

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

# Documentation for Release 10.5(1)

For complete information about this release, refer first to these Release Notes and then refer to the Documentation Guide for Cisco Unified Communications Manager and IM and Presence Service Release 10.5(1) at:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/docguide/10_5_1/CUCM_BK_C2CFB1F8_00_cucm-documentation-guide-1051.html.

# Upgrades

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

# Supported Web Browsers

## Cisco Unified Communications Manager Administration

Cisco Unified Communications Manager Administration supports the following web browsers for Release 10.5(x):

| Platform | Supported Browsers | | |
|---|---|---|---|
| Windows XP | Microsoft Internet Explorer 8 | Mozilla Firefox 10, Firefox 17 ESR | Google Chrome 25 or latest available browser |
| Windows 7 | Microsoft Internet Explorer 9, 10 | Mozilla Firefox 10, Firefox 17 ESR | Google Chrome 25 or latest available browser |
| Windows 8 | Microsoft Internet Explorer 10 | Mozilla Firefox 17 ESR | Google Chrome 25 or latest available browser |
| Windows 8.1 (32 bit) | Microsoft Internet Explorer 10 | Mozilla Firefox 17 ESR | Google Chrome 25 or latest available browser |
| Windows 8.1 (64 bit) | Microsoft Internet Explorer 11 | Mozilla Firefox 17 ESR | Google Chrome 25 or latest available browser |
| Mac Mt-Lion (10.8) | Microsoft Safari 6 | Mozilla Firefox 17 ESR | Google Chrome 25 or latest available browser |

## Cisco Unified Analysis and Reporting and Cisco Unified Serviceability

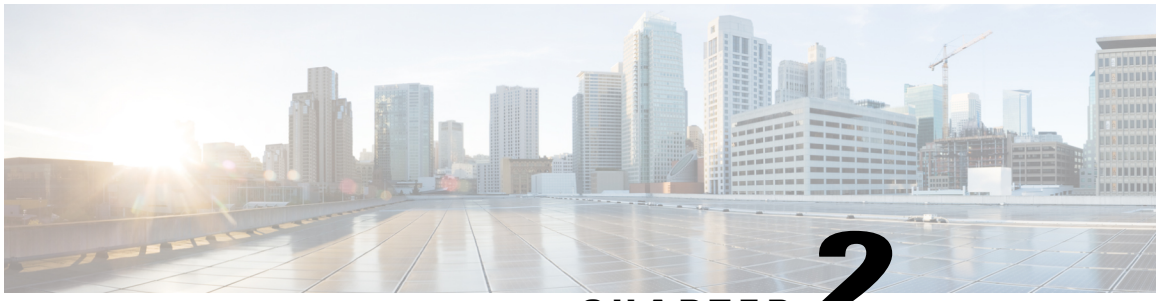
The following table lists the latest supported web browsers for Cisco Unified CDR Analysis and Reporting and Cisco Unified Serviceability for Cisco Unified Communications Manager 10.5(1).

| Platform | Supported Browsers | | |
|---|---|---|---|
| Windows XP | Microsoft Internet Explorer 8 | Mozilla Firefox 24 | Google Chrome 25 or latest available browser |
| Windows 7 | Microsoft Internet Explorer 10 and 11 | Mozilla Firefox 24 | Google Chrome 25 or latest available browser |
| Windows 8 | Microsoft Internet Explorer 10 and 11 | Mozilla Firefox 24 | Google Chrome 25 or latest available browser |
| Mac - Mountain Lion (10.8) | Safari 7 | Mozilla Firefox 24 | Google Chrome 25 or latest available browser |
| Windows 8.1 (64 bit) | Microsoft Internet Explorer 11 | Mozilla Firefox 24 | Google Chrome 25 or latest available browser |
| Windows 8.1 (32 bit) | Microsoft Internet Explorer 10 | Mozilla Firefox 24 | Google Chrome 25 or latest available browser |

# Self Care Portal

Cisco Unified Communications Self Care Portal supports the following web browsers for release 10.5(1).

| Platform | Supported Browsers |
|---|---|
| Windows 7 (32-bit) | Microsoft Internet Explorer 9, 10 |
| Windows 8.1 (32-bit) | Microsoft Internet Explorer 11<br>Firefox 10, Firefox 17 ESR<br>Chrome 25 or latest |
| Mac OS (latest version) | Safari 6 |



CHAPTER 2

# Upgrades


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


## Software Versions

Software Version for IM and Presence Service Release 10.5(1)

- These release notes are based on the following software version: 10.5.1.10000-9.

Software Version for Cisco Unified Communications Manager Release 10.5(1)

- These release notes are based on the following software version: 10.5.1.10000-7.

**Caution** Do not use the Patch Upgrade option when installing Unified Communications Manager, Release 10.5(1). You must install this release by using the bootable ISO image, which you must order through the Product Upgrade Tool.

## Supported Upgrades

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

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

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

# Important Notes about Upgrades

## 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).

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

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

# Upgrade Fails if AXL Password Contains Special Characters

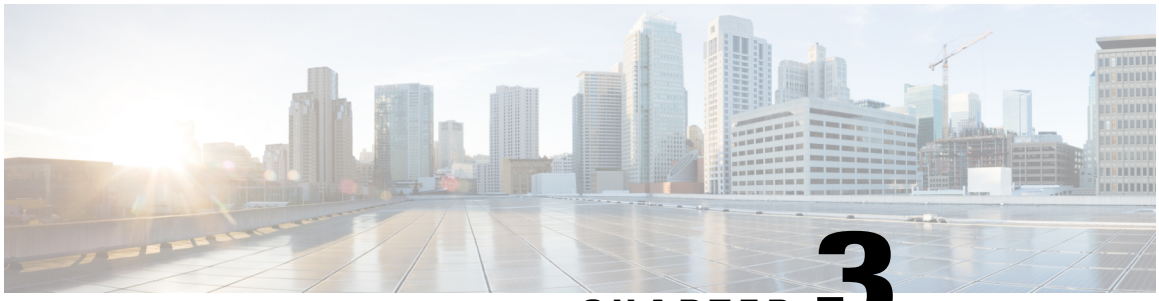
This document update resolves CSCur00547.

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

# OS Administrator Account Required for IM and Presence Upgrades

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

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



CHAPTER 3

# New and Changed Features


- New Default Softkey Templates for Feature Hardkey Phones, page 10
- Cluster-wide Multiserver Certificate Support, page 10
- SAML Single Sign-On, page 19
- SIP Best Effort Early Offer, page 31
- Daylight Saving Time Rules, page 36
- Directory Search in Self Care, page 39
- Embedded Cisco TelePresence Management Suite in Self Care Portal, page 39
- IM and Presence Service Deprecation of Microsoft Exchange Server 2003, page 40
- IM and Presence Service Deprecation of WebDAV , page 40
- IM and Presence Service IPv6 Support, page 40
- IM and Presence Service Support for Encrypted External Database, page 44
- Support Variable Extension Length and +E.164 for LDAP Directory Numbers, page 45
- Voice Gateway Support, page 47
- New CLI Commands, page 51
- Windows 8.1 and Windows Server 2012 R2 Support, page 52
- About Cross-Origin Resource Sharing, page 52
- Configure LDAP Directory, page 53
- New RTMT Alert for Global Dial Plan Replication, page 54
- Silent Monitoring CLI Update, page 55
- Product-Specific Configuration in TelePresence Device User Interfaces, page 55
- Cisco IP Phones and Cisco Desktop Collaboration Experience DX650, page 56

# New Default Softkey Templates for Feature Hardkey Phones

The following softkey templates with new softkey layouts are introduced for Cisco Unified Communications Manager Release 10.5(1):

- Cisco Protected Phone with Feature Hardkeys
- Cisco Chaperone Phone with Feature Hardkeys
- Cisco Feature with Feature Hardkeys
- Cisco User with Feature Hardkeys (default)
- Cisco Manager with Feature Hardkeys
- Cisco Assistant with Feature Hardkeys
- Cisco Shared Mode Manager with Feature Hardkeys

The phones with feature hardkeys have hardkeys for the Hold, Transfer, and Conference call features. The new softkey templates avoid needing both hardkeys and softkeys for these call features.

**Note** The existing Standard User template before Release 10.5(1) appears for both a fresh installation and an upgrade. This is the only built-in template that is appropriate for use on phones that use softkeys for Hold, Transfer, and Conference, such as the Cisco 7961.

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.

**Note** The softkey templates that are added for Cisco Unified Communications Manager Release 10.5(1) support a description length of 100 characters.

**Important** For an upgrade from any version of Cisco Unified Communications Manager before Release 10.5(1), Cisco Unified Communications Manager retains the existing templates from the previous version, and in addition, adds the new softkey templates. It also retains the custom softkey templates (if any) from the previous version. The default template that was used before the upgrade also remains the default template after the upgrade.

# Cluster-wide Multiserver Certificate Support

From Cisco Unified Communications Manager Release 10.5(1), Unified Communications Manager adds support for multiserver certificates which allows the administrator to assign a single certificate for a given certificate unit (for example; Tomcat, CallManager, cup-xmpp, and cup-xmpp-s2s) across multiple servers in a cluster. In Cisco Unified Communications Manager Release 10.0(1) and earlier releases, the system uses a single certificate for each certificate unit on each server in a cluster. As a result of this, the administrator has to configure and maintain a number of security certificates across the deployment. Any application

connecting to the system, including Jabber that validates the certificates to establish a secure connection to the servers, requires that the presented certificates are trusted. If the certificates are not trusted, the system displays a number of security warnings to the users. With signed multiserver certificates in Cisco Unified Communications Manager Release 10.5(1), the system removes these warnings and reduces the number of certificates which the administrator must configure and maintain.

**Note** The administrator can continue to use a single certificate for each certificate unit on each server in a cluster.

The following table describes the basic differences between single-server certificates and multiserver certificates.

***Table 1: Configuration Comparison of Certificates***

| Single-server Certificate | Multiserver Certificate |
|---|---|
| Contains a single Fully Qualified Domain Name (FQDN) or domain in either the Common Name (CN) field or Subject Alternative Name (SAN) extensions. | Contains multiple FQDNs or domains present in SAN extensions. |
| The system uses a single certificate for each server in a cluster. | A single certificate identifies multiple servers. |
| The administrator regenerates the certificate and private key on each individual server in situations such as certificate expiry, and private key compromise. | Because this certificate covers only one public and private key pair common to all servers, it requires secure transfer of same private key to all the servers in a cluster along with the certificate. If the private key is compromised on any server, the certificate and private key must be regenerated for all the servers. |
| Generation of a single-server certificate can add overhead for the administrator in a large cluster because the administrator needs to perform steps such as generate Certificate Signing Request (CSR), send CSR to CA for signing, and upload signed certificate for each of the servers in the cluster. | There is less overhead in managing multiserver certificates, because the administrator performs the steps only once on a given server, and the system distributes the associated private key and signed certificates to all the servers in the cluster. |

# Multiserver Certificate Overview

Subject Alternate Name (SAN) is a section defined under X.509 certificate extensions. SAN contains multiple Fully Qualified Domain Names (FQDN) or hostnames or other valid names. X.509 technology allows placing a trust in the identity of an entity such as an Internet website when it is digitally signed by a Certificate Authority (CA). The identity of a server that is on a network can be qualified by the FQDN and trusted by other clients connecting to this server. The system trusts the server because it presents an X.509-based certificate that is signed by a CA. The certificate allows the hostname or the FQDN to be included in either the Subject Name field of the certificate or the SAN field of the certificate, or in both the fields of the certificate.

The SAN field allows multiple FQDNs, domain names, or other approved names to be included in X.509 certificates so that a user does not need to generate a certificate for each server. Instead one certificate identifies multiple servers.

Unified Communications Manager supports a single CA signed certificate with SAN extensions across multiple servers for each of the Tomcat, CallManager, and IM and Presence Service services. The SAN fields are utilized and shared across multiple servers in a cluster for each of the Tomcat, CallManager, cup-xmpp, and cup-xmpp-s2s certificates. The administrator selects between single-server certificates and multiserver certificates with SAN extensions to generate a CSR, and then uploads the certificate or certificate chain.

## Multiserver Certificate Benefits

- Allows the administrator to configure the Common Name (CN) field of the certificate.
- Allows the administrator to generate a single CSR, sign a single certificate, and upload a single certificate for each service.
- Provides secure transfer of private key and CA signed certificate across all the servers in a cluster by using the Platform Administrative Web Services (PAWS) API.

The following table lists the certificate names and the servers where the respective private key and certificates are copied.

***Table 2: Certificate Names and Servers***

| Certificate | Server | Certificate usage |
|---|---|---|
| Tomcat | • Unified Communications Manager<br>• IM and Presence Service | Any applications, including Jabber clients accessing Cisco Tomcat service, use this certificate to verify the Unified Communications Manager server and IM and Presence Service server identity. |
| CallManager | Unified Communications Manager | Any applications, endpoints and Jabber clients accessing CallManager service use this certificate to verify the Unified Communications Manager server identity. |
| cup-xmpp | • IM and Presence Service | Jabber clients and Cisco AJAX XMPP Library (CAXL) clients use this certificate to verify the IM and Presence Service server identity. |
| cup-xmpp-s2s | • IM and Presence Service | This certificate is used to establish secure server-to-server connections for the IM and Presence Service XMPP interdomain federation feature. |

While generating the CSR, the administrator has the option of configuring the CN field or leaving the default value of CN for Tomcat, cup-xmpp, cup-xmpp-s2s, and CallManager (single-server or multiserver) certificates. However, the administrator cannot modify the CN for self-signed certificates. The CN has a default value assigned to it.

The default value of CN will be FQDN (if domain name is configured) or hostname (if domain name is not configured) of the server from which the request is generated for single-server or SAN-based multiserver CSR.

**Note** The administrator can configure the SAN field to add more FQDNs or domain names.

The following table lists the SAN entries for each of the certificate types.

***Table 3: Certificates and SAN Entries***

| Certificate | SAN Entries | |
|---|---|---|
| | **CSR (Single-Server)** | **CSR (Multiserver)** |
| Tomcat | • FQDN (or hostname)<br>• Network domain (if configured) | • FQDN of all Unified Communications Manager and IM and Presence Service servers in the cluster<br>• Network domains (if configured)<br>• Custom values |
| CallManager | • FQDN (or hostname)<br>• Network domain (if configured) | • FQDN of all Unified Communications Manager servers in the cluster<br>• Network domains (if configured)<br>• Custom values |
| cup-xmpp | • FQDN (or hostname)<br>• Presence domains | • FQDN of all IM and Presence Service servers in the cluster<br>• Presence domains: Configure Presence domains by using the **IM and Presence Server Administration** window, and selecting **Presence** > **Domains**.<br>• Custom values |

| Certificate | SAN Entries | |
|---|---|---|
| | CSR (Single-Server) | CSR (Multiserver) |
| cup-xmpp-s2s | • FQDN (or hostname)<br>• Presence domains<br>• Wildcarded Presence domains (if configured)<br>• Email domains<br>• Group Chat Server Alias | |

| Certificate | SAN Entries | |
|---|---|---|
| | CSR (Single-Server) | CSR (Multiserver) |
| | | • FQDN of all IM and Presence Service servers in the cluster<br>• Presence domains: Configure Presence domains by using the **IM and Presence Server Administration** window, and selecting **Presence** > **Domains**.<br>• Wildcarded Presence domains (if configured): Enable or disable this feature by using the **IM and Presence Server Administration** window, and selecting **Presence** > **Settings** > **Standard Settings**.<br>• Email domains (if configured):<br>◦ Enable or disable the feature by using the **IM and Presence Server Administration** window, and selecting **Presence** > **Settings** > **Standard Settings**.<br>◦ Configure Email domains by using the **IM and Presence Server Administration** window, and selecting **Presence** > **Inter-Domain Federation** > **Email Federated Domains**.<br>• Group Chat Server Alias: Configure Group Chat Server Aliases by using the **IM and Presence Server Administration** window, and selecting **Messaging** > **Group Chat Server Alias Mapping**. |

| Certificate | SAN Entries | |
|---|---|---|
| | CSR (Single-Server) | CSR (Multiserver) |
| | | • Custom values |

The following is an example of a Tomcat certificate setup:

- Network domain is *cisco.com*
- Nodes in the cluster are *cucm-node-01, cucm-node-02, cup-node-03*
- Email domain is *email.com*

The network domain and cluster server FQDNs are included in the CSR and subsequent signed certificate by default. The email domain must be manually added as a custom additional SAN entry. The SAN in the Tomcat certificate appears as follows:

```
Subject Alternative Names:
DNS: cucm-node-01.cisco.com, DNS: cucm-node-02.cisco.com,
DNS:cup-node-03.cisco.com, DNS: cisco.com, DNS: email.com
```

Depending on the system configuration, Jabber users who connect to the system can enter their user ID as *user@email.com*. Establishment of the secure connection and validation of the Tomcat X.509 certificate is dependent on the values in the SAN extension.

## Manage Certificates

The following topics describe the functions that you can perform for single-server and multiserver certificates from the Certificate Management menu.

Restart the following services after regenerating or uploading single-server certificates:

***Table 4: Services to Restart for Single-Server Certificates***

| Certificate | Services to Restart |
|---|---|
| CallManager | Cisco CallManager Service, Cisco TFTP Service, and all other relevant services that use CallManager certificate. |
| cup-xmpp | Cisco XCP Router |
| cup-xmpp-s2s | Cisco XCP XMPP Federation Connection Manager |

Restart the following services after regenerating or uploading multiserver certificates with SAN extensions:

*Table 5: Services to Restart for Multiserver Certificates with SAN Extensions*

| Certificate | Services to Restart |
|---|---|
| CallManager (Restart on each Unified Communications Manager server) | Cisco CallManager Service, Cisco TFTP Service, and all other relevant services that use CallManager certificate. |
| cup-xmpp (Restart on each IM and Presence server) | Cisco XCP Router |
| cup-xmpp-s2s (Restart on each IM and Presence server) | Cisco XCP XMPP Federation Connection Manager |
| Tomcat (Restart on each Unified Communications Manager and IM and Presence server | Cisco Tomcat on all the servers in the cluster |

**Note** A new section "Configure Multiserver Certificate" has been added to *Cisco Unified Communications Operating System Administration Guide*.

Configure Multiserver Certificate, on page 17

**Note** Cisco Unified Communications operating system generates multiserver certificates with SAN extensions for the Tomcat service, CallManager service, and IM and Presence Service.

For information on configuring multiserver certificates, see the *Cisco Unified Communications Operating System Administration Guide* that supports this release.

### IM and Presence Service Multiserver Certificates

For more information on Security Certificate management on IM and Presence Service, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager, Release 10.5(1)* and the *Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager, Release 10.5(1)*.

## Configure Multiserver Certificate

Cisco Unified Communications operating system generates multiserver certificates with SAN extensions for the Tomcat service, CallManager service, and IM and Presence Service.

The following procedure provides an overview of this process.

**Note** The detailed steps are explained in subsequent sections.

### Procedure

**Step 1** Log in to Cisco Unified Communications Operating System Administration on any Unified Communications Manager or IM and Presence Service server using your administrator password.

**Step 2** Generate a CSR on the server.

**Note** Cisco Unified Communications Operating System Administration allows the system administrator to select the distribution type when generating a CSR for the individual certificate purposes that supports the multiserver option. The system automatically populates the CSR with the required SAN entries and displays the default SAN entries on the screen. On generating a multiserver CSR, the system automatically distributes that CSR to all the required servers in the cluster. For details about certificate names and servers, see Table 2: Certificate Names and Servers, on page 12.

**Step 3** Download the CSR to your PC.

**Step 4** Use the CSR to obtain an application certificate from a CA and request that the CA sign the CSR.

**Note** Get information about obtaining a root certificate from your CA.

**Step 5** Obtain the root CA certificate or certificate chain to upload on the cluster.

**Note** Get information about obtaining a root certificate from your CA.

**Step 6** Upload the root CA certificate and signed CA certificate to the server.
During upload, the system automatically distributes the certificates to all the required servers in the cluster.

**Step 7** Restart the services that are affected by the new certificate.

**Tip** For all certificate types, restart the corresponding service (for example, restart the Cisco Tomcat service after regenerating the Tomcat certificate).

**Note** For details about the corresponding service names for each of the certificate types, see Table 5: Services to Restart for Multiserver Certificates with SAN Extensions, on page 17.

See the *Cisco Unified Communications Manager Serviceability Administration Guide* for information about restarting services.

## Generate Certificate Signing Request for Multiserver Certificate

**Note** If your deployment contains Cisco Unified Communications Manager and IM and Presence Service nodes that are installed on different network domains, you should generate the multiserver Tomcat certificate from the Unified Communications Manager node. This action ensures that the Unified Communications Manager network (parent) domain appears in the certificate.

You must generate a new certificate signing request when you want to renew a multiserver certificate.

### Procedure

**Step 1** Select **Security** > **Certificate Management**.

The **Certificate List** window appears.

**Step 2** Use the Find controls to filter the certificate list.

**Step 3** Click **Generate CSR**.
The **Generate Certificate Signing Request** window appears.

**Step 4** From the **Certificate Purpose** drop-down list, select the required certificate purpose.

**Step 5** From the **Distribution** drop-down list, select **Multi-server (SAN)**.

**Note** The Multi-server (SAN) option is available only when you select either Tomcat, CallManager, cup-xmpp or cup-xmpp-s2s from the **Certificate Purpose** drop-down list.

**Note** By default, the system populates the CN field with the server FQDN (or hostname). You can modify the value, if required. For self-signed certificate, the CN is not configurable.

**Step 6** From the **Key Length** drop-down list, select **1024** or **2048**.

**Step 7** From the **Hash Algorithm** drop-down list, select **SHA1** or **SHA256**.

**Step 8** Click **Generate** to generate a new CSR.

**Note** The new CSR that is generated for a specific certificate type overwrites any existing CSR for that type. The CSR is automatically distributed to all the required servers in the cluster.

See Table 2: Certificate Names and Servers, on page 12 to get the list of the certificate names and the servers where the respective private key and certificates are copied.

### Download Certificate Signing Request for Single-Server and Multiserver Certificate

#### Procedure

**Step 1** Select **Security** > **Certificate Management**.
The **Certificate List** window appears.

**Step 2** From the list, click the Common Name of the entry with the type **CSR Only** and a Distribution value matching the Common Name.

**Note** For the multiserver SAN certificate, click the Common Name of the entry with type **CSR Only** and a Distribution value of **Multi-Server (SAN)**.

The **CSR Details** window appears.

**Step 3** Click **Download CSR**.

**Step 4** After the CSR download completes, click **Close**.

# SAML Single Sign-On

The following content has been added to the "SAML Single Sign-On counters" table in the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Cisco Unified Communications Manager Release 10.5(1) supports SAML-based Single Sign-On. Unified RTMT displays seven additional counters that are functional in Cisco Unified Communications Manager Release 10.5(1).

**Note** In Cisco Unified Communications Manager Release 10.0(1), SAML_REQUESTS and SAML_RESPONSES are the only two counters that are functional and are displayed in the Unified RTMT.

The following table contains information about SAML Single Sign-On counters.

***Table 6: SAML Single Sign-On Counters***

| Counter | Counter Description |
|---|---|
| SAML_FAILED_REQUESTS | This counter represents the number of failed or invalid SAML requests.<br>**Tip** For details on the exact failures, see one of the following logs:<br>• `ssosp000xx.log`<br>• `ssoApp.log` |
| SAML_FAILED_RESPONSES | This counter represents the number of failed or invalid SAML responses received from the configured Identity Provider.<br>**Tip** For details on the exact failures, see one of the following logs:<br>• `ssosp000xx.log`<br>• `ssoApp.log` |
| OAUTH_TOKENS_ISSUED | This counter represents the number of OAuth tokens that are issued by the administrator. |
| OAUTH_TOKENS_ACTIVE | This counter represents the number of OAuth tokens that are currently active in the Token store. |
| OAUTH_TOKENS_VALIDATED | This counter represents the number of times OAuth tokens are validated. |
| OAUTH_TOKENS_EXPIRED | This counter represents the number of OAuth tokens that are removed from the Token store upon expiry. |
| OAUTH_TOKENS_REVOKED | This counter represents the number of OAuth tokens that are revoked by the administrator. |

**Note** When a user requests a new token from the same client, the existing token is lost and is no longer valid. The authorization service issues a new token that replaces the previous token. The token that is lost or replaced is not registered in any of the available counters.

The following content has been added to the "SAML Single Sign-On" chapter in the *Features and Services Guide for Cisco Unified Communications Manager*.

### SAML Single Sign-On

After you enable SAML Single Sign-On (SSO), users will be able to access the following web applications without logging in again:

- Cisco Unified Communications Manager Administration
- Cisco Unified Reporting
- Cisco Unified Serviceability
- Unified Communications Self Care Portal

### Enable SAML SSO

**Note** After you enable SAML SSO, you can log in to the following applications directly from the default page:

- Cisco Unified Reporting
- Cisco Unified Serviceability

# JTAPI Support for Single Sign-On

**Note** The following information is for JTAPI developers.

With Cisco Unified Communications Manager Release 8.5(1), JTAPI can authenticate applications using Single Sign-On (SSO) Tickets and with Unified Communications Manager Release 10.0(1), JTAPI can also authenticate applications using an SSO Cookie.

With Unified Communications Manager Release 10.5(1), JTAPI expands SSO support to include authentication using a standards-based SAML Oauth token.

Single Sign-On provides the following advantages:

- Simplifies access
- Centralizes Credential Management
- Eliminates password resets
- Is secure

- Integrates with Multivendor Identity Provider (IdP)

### Details

- SSO is a cluster-wide setting that can be enabled after an installation or upgrade to Release 10.5(1).
- Application user login procedure does not change. JTAPI Applications using Application accounts can only log in with username and password.
- Applications using LDAP Synchronized User accounts can log in with either username and password or Oauth token when SSO is enabled.
- Oauth token authentication is not supported for locally configured user accounts.
- JTAPI supports the use of an SSO Oauth token for both secure and non-secure connections.
- The application must provide the SSO Oauth token in the providerString for initializing and receiving the Provider object.

A JTAPI provider is established using the method getProvider(String provStr) on a JtapiPeer object. The mode of authentication is governed by the format of the provider string, which is passed as an argument to this method.

**General format**

**username/password authentication:**

serverIP;login=<userName>;passwd=<password>;

For example:

John/Cisco123

serverIP;login=John;passwd=Cisco123;

**SSO Oauth token authentication:**

severIP;ssooauthtoken=<oAuthToken>;

For example:

token “abcde”

serverIP;ssooauthtoken=abcde;

### Sample Code

```
//application gets SSOoAuthToken
String oAuthToken = tokenFetchedByApp;
//Create provider string in the required format
String providerString = ctiserverIP + “;ssooauthtoken=” + oAuthToken +”;”;
JtapiPeer peer = JtapiPeerFactory.getJtapiPeer ( null );
try {
         Provider provider = peer.getProvider (providerString);
} catch (Exception exp ){
//Exception handling code
}
```

## Acquire the Single Sign-On Token

Complete the following procedure to acquire the Single Sign-On (SSO) Oauth token.

### Procedure

**Step 1** Determine the SSO feature status. Applications should use the following URL to determine whether the SSO feature is enabled.
For example: https://<anyPublisherOrSubscriberIP>:8443/ssosp/ws/public/singlesignon.
The response <Status enabled="true"/> indicates if SSO is enabled. <anyPublisherOrSubscriberIP> is the IP address of any Unified Communications Manager Publisher or Subscriber node.

**Result**:

```
<SSOResult>
<ErrorCode>0</ErrorCode>
<Response>
<SingleSignOn version="10.5.0.98000-77">
<Status enabled="true"/>
<Token reuse="false"/>
<Uri>https://<anyPublisherOrSubscriberIP>:8443/ssosp/oauth/authorize</Uri>
</SingleSignOn>
</Response>
</SSOResult>
```

**Step 2** If the SSO status = true, parse the <URI> response and add the mandatory parameters: https://<anyPublisherOrSubscriberIP>:8443/ssosp/oauth/authorize.

**Supported Parameters:**

response_type=token (mandatory) Value *must* be 'token' in Unified Communications Manager Release 10. If a client passes a value other than 'token', the request is rejected with the error 'unauthorized_client'.

client_id=C45c61cee396bcce508c58f1eefe326685c85243edf77f491d631e7b01d677f94 (mandatory) JTAPI applications *must* pass this OAuth client_id. UC 10.0 does not support client_id registration, so all JTAPI applications will use "C45c61cee396bcce508c58f1eefe326685c85243edf77f491d631e7b01d677f94". If an unrecognized client_id is passed, the request is rejected with the error 'unauthorized_client'.

**Example:**
https://10.10.10.10:8443/ssosp/oauth/authorize?
response_type=token&client_id=C45c61cee396bcce508c58f1eefe326685c85243edf77f491d631e7b01d677f94
&token_type=Bearer

**Step 3** Obtain an Oauth token by issuing a request through a WebView/Browser.
Redirection to the IDP occurs automatically from the /ssosp/oauth/authorize API. Enter your password and the token is returned to the WebView/Browser.

**Result:**
Within the browser/webview, the connecting client is redirected to the redirect_uri with the OAuth access token as a parameter.

**Step 4** After successfully authenticating, parse the 'access_token' value from the response. Copy the entire value for access_token up to the '&'. This token is used in the getProvider (providerString) for the 'ssooauthtoken' parameter.
**Result:**
https://10.10.10.10:8433/ssosp/publicoauthcb#access_token=
Mjo4YFiNTJmNy1JyZRmLTRjMTQtYTNmMy1jNDgyYzQ2NjcyOGM&token_type=Bearer&expires_in=3600

Access token from the result above: Mjo4YFiNTJmNy1JyZRmLTRjMTQtYTNmMy1jNDgyYzQ2NjcyOGM

## Interface Changes for Single Sign-On Oauth Support

### Interface CiscoJtapiException

Three new fields are added in CiscoJtapiException for SSO Oauth support.

### Declaration

public interface CiscoJtapiException

### Fields

***Table 7: Fields in public static final int***

| Interface | Field | Description |
|---|---|---|
| public static final int | CTIERR_OAUTH_TOKEN_UNAUTHORIZED | This error code is returned if the Oauth token is expired and the application tries to reopen provider with same oauth token. |
| public static final int | CTIERR_INVALID_OAUTH_TOKEN | This error code is returned if the Oauth token is invalid. |
| public static final int | CTIERR_OAUTH_SERVER_NOT_REACHABLE | This error code is returned if the Oauth server is not reachable for validation. |

## Use Cases for Single Sign-On Oauth Support

***Table 8: Successful Authentication Using an SSO Oauth Token***

| Action | Event | Result |
|---|---|---|
| Application tries to open the provider with a valid SSOOauthToken<br>JtapiPeer.getProvider("ServerIP;ssooauthtoken=<<br>ssoOauthTokenfromAD>";); | ProvInServiceEv | Provider object is returned to application. |

*Table 9: Valid SSO Oauth Token with a UserId and Password*

| Action | Event | Result |
|---|---|---|
| Application tries to open the provider with a valid SSOOauthToken along with UserId and Password<br>JtapiPeer.getProvider("ServerIP;login=<br><UserId>;passwd=<br><password>ssooauthtoken=<<br>ssoOauthTokenfromAD>";); | ProvInServiceEv | Provider object is returned to application. But the authentication is done based on ssooauthtoken and the userid and password are ignored by JTAPI. |

*Table 10: Application Specifies Invalid Oauth Token but a Correct Userid and Password in API*

| Action | Event | Result |
|---|---|---|
| Application specifies invalid token but correct userid and password in API<br>JtapiPeer.getProvider("ServerIP;login=<br><UserId>;passwd=<br><password>ssooauthtoken=<<br>ssoOauthTokenfromAD>";); | PlatformException | getErrorCode() = CiscoJtapiException.<br>CTIERR_INVALID_OAUTH_TOKEN |

*Table 11: Application Specifies an Empty Oauth Token*

| Action | Event | Result |
|---|---|---|
| Application tries to open the provider with an empty SSOOauthToken<br>JtapiPeer.getProvider(ServerIP;ssooauthtoken=<<br>ssoOauthTokenfromAD >;); | PlatformException | getErrorCode() = CiscoJtapiException.<br>CTIERR_INVALID_PARAMETER |

*Table 12: Application Specifies an Invalid Token*

| Action | Event | Result |
|---|---|---|
| Application tries to open the provider with an empty SSOOauthToken<br>JtapiPeer.getProvider(ServerIP;ssooauthtoken=<<br>Any Invalid Token>;); | PlatformException | getErrorCode() = CiscoJtapiException.<br>CTIERR_INVALID_OAUTH_<br>TOKEN |

***Table 13: Application Tries to Open the Provider with Oauth Token but OauthServer Is Not Reachable by the CTI for Validation***

| Action | Event | Result |
|---|---|---|
| Application tries to open the provider with an SSOOauthToken<br>JtapiPeer.getProvider(ServerIP;ssooauthtoken=<<br>Any Invalid Token>;); | PlatformException | getErrorCode() = CiscoJtapiException.<br>CTIERR_OAUTH_SERVER_<br>NOT_REACHABLE |

***Table 14: Failover Scenario***

| Action | Event | Result |
|---|---|---|
| Application tries to open the provider with a valid SSOOauthToken<br>JtapiPeer.getProvider("ServerIP;ssooauthtoken=<<br>ssoOauthTokenfromAD >;");<br>CTI failover happens | ProvInServiceEv<br>ProvOutOfServiceEv<br>ProvInServiceEv | Provider object is returned to application.<br>ProvOutOfServiceEv is reported to the application for current CTI node.<br>JTAPI will connect to the next CTI node with the same SSO Oauth token as used earlier since that token has not expired.<br>If the token has expired for the next open provider then the application has to re-initialize the JTAPI with a fresh Oauth token. |

***Table 15: Successful Authentication Using an SSO Oauth Token for Secured Scenario***

| Action | Event | Result |
|---|---|---|
| Application tries to open the provider with a valid SSOOauthToken, Fully Qualified Directory Name of client certificate, and the server certificate<br>JtapiPeer.getProvider("ServerIP;ssooauthtoken=<br><ssooauthtokenfromAD>;ClientCert=<FQDN client<br>certificate>;ServerCert=< FQDN servercertificate >" | ProvInServiceEv | Secured connection is set up between JTAPI and CTI node.<br>Provider object is returned to application. |

# TAPI Support for Single Sign-On

**Note** The following information is for TAPI developers.

With Cisco Unified Communications Manager Release 10.5(1), the Cisco TSP client is enhanced to support authentication using Single Sign-On (SSO).

Using Single Sign-On provides the following advantages:

- Simplifies access
- Centralizes Credential Management
- Eliminates password resets
- Is Secure
- Integrates with Multivendor Identity Provider (IdP)

The Cisco TSP client can be configured to use either a static password, as in previous releases, or to use Single Sign-On.

If the Cisco TSP client is configured to use an Application Account or a local User account, configure the password in the client.

If the Cisco TSP client is configured to use an LDAP Synchronized User Account and Single Sign-On is enabled for the Cisco Unified Communications Manager cluster, choose Single Sign-On.

When Single Sign-On is selected and the TAPI application is opened, the Cisco TSP client automatically attempts to acquire the OAuth token needed to access CTI Manager. For a first-time login and when the token expires, a browser window appears asking the user to provide Single Sign-On credentials.

### UI Enhancements for Cisco TSP-Installer

TSP Notifier is now a required component and is installed automatically during a fresh installation or upgrade regardless of SSO settings. For each desired TSP Instance, the CiscoTSP Installer UI is enhanced to allow the user to select either Single Sign-On or Username/Password as the authentication type during a fresh installation.

The default authentication type for a fresh installation is Single Sign-On.

You can select **Use the following Credentials** to change the authentication type to Username/Password from SSO.

If you want to change the authentication type after installation is complete, access the Cisco TSP Configuration-User Tab UI and select the authentication type you want to use.

During an upgrade of an older Cisco TSP client to a new Cisco TSP client, the authentication type of the end user is retained from the previous configuration of the CiscoTSP client that is being upgraded.

If you choose to add a fresh TSP instance during the upgrade, the newly added TSP instance is completely configurable and you can select the authentication type as either SSO or Username\Password.

### Silent Installation

The new parameter **AUTH** is added to the existing Silent Install Command line, to specify Authentication type during installation.

### Examples

Customer information:

- USER ID = bob
- PASSWORD = cisco123

CTI-Manager configuration:

- CTIManager1= 1.1.1.1 (ipv4) , 1:1:1:1:1:1 (ipv6), cti-dev-94.cisco.com (hostname)
- CTI1_TYPE = Ipv4 , Ipv6 , Host

#### Authentication Type: User Credentials

Silent install for end user : bob with Authentication Type : User Credentials , Primary CTIManager IP address : 1.1.1.1 and IP addressing mode : IPV4

- Command Line for a 32-bit machine : **CiscoTSP.exe /s /v"/qn AUTH=0 PASS=cisco123 USER=bob CTI1**= CTIManager address **CTI1_TYPE=IPV4"**
- Command Line for a 64-bit machine : **CiscoTSPx64.exe /s /v"/qn AUTH=0 PASS=cisco123 USER=bob CTI1=1.1.1.1 CTI1_TYPE=IPV4"**

Silent install for end user : bob with Authentication Type : User Credentials , Primary CTIManager IP address : 1:1:1:1:1:1 and IP addressing mode : IPV6

- Command Line for a 32-bit machine : **CiscoTSP.exe /s /v"/qn AUTH=0 PASS=cisco123 USER=bob CTI1**= CTIManager address **CTI1_TYPE=IPV6"**
- Command Line for a 64-bit machine :**CiscoTSPx64.exe /s /v"/qn AUTH=0 PASS=cisco123 USER=bob CTI1=1.1.1.1 CTI1_TYPE=IPV6"**

#### Authentication Type: Single Sign On

Silent install for end user : bob with Authentication Type : Single Sign On, Primary CTIManager IP address : 1.1.1.1 and IP addressing mode : IPV4

- Command Line for a 32-bit machine : **CiscoTSP.exe /s /v"/qn AUTH=1 CTI1=1.1.1.1 CTI1_TYPE=IPV4"**
- Command Line for a 64-bit machine : **CiscoTSPx64.exe /s /v"/qn AUTH=1 CTI1=1.1.1.1 CTI1_TYPE=IPV4"**

Silent install for end user : bob with Authentication Type : Single Sign On, Primary CTIManager IP address: 1:1:1:1:1:1 and IP addressing mode : IPV6

- Command Line for a 32-bit machine : **CiscoTSP.exe /s /v"/qn AUTH=1 CTI1=1.1.1.1.1.1 CTI1_TYPE=IPV6"**
- Command Line for a 64-bit machine : **CiscoTSPx64.exe /s /v"/qn AUTH=1 CTI1=1.1.1.1.1.1 CTI1_TYPE=IPV6"**

Silent install for end user : bob with Authentication Type : Single Sign On , Primary CTIManager IP address : cti-dev-94.cisco.com and IP addressing mode : Hostname

- Command Line for a 32-bit machine : **CiscoTSP.exe /s /v"/qn AUTH=1 CTI1=cti-dev-94.cisco.com CTI1_TYPE=HOST"**
- Command Line for a 64-bit machine : **CiscoTSPx64.exe /s /v"/qn AUTH=1 CTI1=cti-dev-94.cisco.com CTI1_TYPE=HOST"**

For more information about Silent Installation, see “Silent Installation of Cisco Unified CM TSP” in the *TAPI Developer Guide*.

### Limitations

Authentication using a Single Sign-On is not supported when multiple instances of TSP are configured.

Users must log out of the operating system when they switch accounts (for example, Microsoft switch user feature is not supported).

### Interface Changes

The following messages can appear in the tool tip box of CiscoTSPNotifier when failures occur:

- Unified CM TSP SSO OAUTH Authentication failed – Token Unauthorized
- Unified CM TSP SSO OAUTH Authentication failed – Invalid Token
- Unified CM TSP SSO OAUTH failed – Server is not Reachable
- Unified CM TSP SSO OAUTH Fetch failed – SSO is Disabled on Server
- Unified CM TSP SSO OAUTH Fetch failed – OAUTH Invalid message
- Unified CM TSP SSO OAUTH Fetch failed – Receive TimeOut
- Unified CM TSP SSO OAUTH Fetch failed – SSO Status
- Unified CM TSP SSO OAUTH Fetch failed – SSO Token

## TAPI Use Cases for Single Sign-On Support

The following are TAPI use cases for Single Sign-On Support.

***Table 16: Successful Authentication Using an SSO OAuth Token***

| Action | Result |
|---|---|
| 1 The application performs LineInitialize().<br>2 Provide the correct user credentials in the popup window. | The dialog automatically closes and an OAuth Token is acquired. The application connects to CTI and the provider opens. |

***Table 17: Provider Opens When SSO OAuth Token Is Already Present***

| Action | Result |
|---|---|
| The application performs LineInitialize(). | Application connects to CTI and the provider opens. |

*Table 18: Change Authentication Method From Username and Password to SSO*

| Action | Result |
|---|---|
| 1 The application performs LineInitialize().<br>2 Change the authentication method to SSO.<br>3 Provide the correct user credentials in the popup window. | The dialog automatically closes and the OAuth Token is acquired. The application connects to CTI and the provider opens. |

*Table 19: Failover Scenario*

| Action | Result |
|---|---|
| 1 The application performs LineInitialize().<br>2 Provide the correct user credentials in the popup window.<br>3 Stop the CTI Manager of the publisher. | TSP automatically connects to the subscriber (using the SSO Oauth token already acquired).<br>Failover to the backup node occurs. |

*Table 20: Successful Authentication Using an SSO OAuth Token for a Secured Scenario*

| Action | Result |
|---|---|
| 1 The application performs LineInitialize().<br>2 Provide the correct user credentials in the popup window. | The dialog automatically closes and the OAuth Token is acquired. The application connects to CTI through a secure connection and Provider opens. |

*Table 21: Provider Opens When Notifier Is Not Running*

| Action | Result |
|---|---|
| The application performs LineInitialize(). | The TSP LineInitialize() fails with proper error. (Failure is permanent.) |

*Table 22: Provider Opens Without Providing User Credentials*

| Action | Result |
|---|---|
| 1 The application performs LineInitialize().<br>2 Do not provide any credentials in the popup window and wait for some time. | TSP notifier sends an error to the TSP and then the TSP retrys the connection.<br>TSPNOTIFIER_ERR_OAUTH_TOKEN_FETCH_FAILURE (Failure is temporary.) |

*Table 23: Provider Opens with Invalid User Credentials*

| Action | Result |
|---|---|
| 1 The application performs LineInitialize().<br>2 Provide invalid user credentials in the popup window. | A new popup window appears.<br>"Invalid user credentials" error message appears. |

*Table 24: Provider Opens Using SSO on a Cisco Unified Communications Manager Where SSO Is Not Enabled*

| Action | Result |
|---|---|
| The application performs LineInitialize(). | The provider fails to open and the error message "SSO is not enabled on the CUCM" appears. |

*Table 25: SSO OAuth Token Expires After CTIManager Failover Fallback*

| Action | Result |
|---|---|
| 1 The application does a LineInitialize().<br>2 Provide the correct user credentials in the popup window.<br>3 Wait for the SSO OAuth token to expire.<br>4 Stop the CTI Manager of the publisher. | Application automatically connects to the CTI Manager of the subscriber and the popup window appears requesting credentials because the token has expired. |

# Web Dialer Single Sign-On Support

With Release 10.5(1), the Web Dialer interface supports Single Sign-On (SSO). After you activate SSO on the cluster, Web Dialer SSO is enabled along with all other web applications that support SSO. For more information about activating Single Sign-On, see the *Features and Services Guide for Cisco Unified Communications Manager*.

Applications that use Web Dialer interface are backward compatible with earlier releases of Cisco Unified Communications Manager. They may use SSO or continue to use Username and Password, independent of SSO. For more information about using the Web Dialer interface with Single Sign-On, go to: `http://developer.cisco.com/web/webdialer`.

# SIP Best Effort Early Offer

SIP Early Offer means media negotiation is initiated in the SIP INVITE request and concluded in the 200 OK response. Delayed Offer means media negotiation is initiated in the 200 OK response and concluded in the

subsequent ACK request. Although support for Delayed Offer is mandated by IETF RFC 3261, some SIP products cannot respond appropriately to Delayed Offer.

Early Offer requires a complete session description, which may not be available at the time of the INVITE request.

Cisco Unified Communications Manager Release 10.5(1) provides the following configuration options for SIP Early Offer support:

- Early Offer Mandatory—Early Offer is always sent. Accordingly, an MTP will be inserted to provide a complete session description protocol (SDP) at the time of outbound INVITE if calling-side media information is unavailable. When calling-side media information is available, an MTP will not be inserted. This configuration option is part of the existing Early Offer support for voice and video calls.
- Best Effort Early Offer—Does not insert an MTP but sends a Delayed Offer INVITE if a complete session description is not available.
- Early Offer Disabled—In this case, Delayed Offer is used exclusively.

The following table provides an overview of the interactions between the different configuration options.

***Table 26: Configuration Interactions***

| SIP Profile Early Offer Support Configuration | Calling-Side Media Information Available? | MTP Inserted? | Outbound INVITE |
|---|---|---|---|
| Early Offer Mandatory | No | Yes | Early Offer |
| Early Offer Mandatory | Yes | No | Early Offer |
| Best Effort Early Offer | No | No | Delayed Offer |
| Best Effort Early Offer | Yes | No | Early Offer |
| Early Offer Disabled | No | No | Delayed Offer |
| Early Offer Disabled | Yes | No | Delayed Offer |

The following sections include the benefits of Best Effort Early Offer, the modified SIP trunk setup procedure, and the new settings that have been added to the SIP Profile.

# SIP Best Effort Early Offer Benefits

Best Effort Early Offer on a SIP trunk allows a SIP trunk to send an Early Offer without inserting an MTP, while preserving the ability of the SIP trunk to fallback to Delayed Offer when calling-side media information is unavailable at the time of outbound INVITE. The insertion of a media termination endpoint (MTP) is avoided, in this case.

Best Effort Early Offer provides the following benefits:

- Best Effort Early Offer on a SIP ICT preserves the capability of the destination cluster to send an Early Offer without inserting an MTP. For example, if cluster A sends an Early Offer, the destination cluster

of the SIP trunk (cluster B) can send an Early Offer on another SIP trunk without inserting an MTP, the same behavior as the Early Offer Mandatory configuration option. With the new Best Effort Early Offer setting, if cluster A sends a Delayed Offer on the SIP trunk, cluster B can send a Delayed Offer and not insert an MTP. In contrast, If the outbound SIP trunk on cluster B is configured as Early Offer Mandatory, cluster B is forced to insert an MTP to make an Early Offer.

- Best Effort Early Offer avoids premature MTP insertion in cases where it may not be necessary.
- Best Effort Early Offer preserves video and secure media in cases where MTP insertion is not necessary.
- Best Effort Early Offer provides the best interoperability with the least MTP usage.

# Set Up SIP Trunk

### Procedure

**Step 1** Choose **Device** > **Device Settings** > **SIP Profile** and select an existing SIP profile.

**Step 2** Copy the SIP profile.

**Step 3** In the **Name** field, enter a new name for the profile.

**Step 4** From the **Early Offer support for voice and video calls** drop-down list, choose one of the following:

- Disabled (Default value)
- Best Effort (no MTP inserted)
- Mandatory (insert MTP if needed)

**Step 5** Click **Save**.

**Step 6** Choose **Device** > **Trunk** and choose the SIP profile you want to assign to a SIP Trunk.

**Step 7** From the **Trunk Configuration** window, click **Reset**.

# SIP Profile Settings

The following field has been added for the SIP Best Effort Early Offer feature.

| Field | Description |
|---|---|
| Early Offer support for voice and video calls | This field configures Early Offer support for voice and video calls. When enabled, Early Offer support includes a session description in the initial INVITE for outbound calls. Early Offer configuration settings on SIP profile apply only to SIP trunk calls. These configuration settings do not affect SIP line-side calls. If this profile is shared between a trunk and a line, only a SIP trunk that uses the profile is affected by these settings.<br><br>Because End to End RSVP provides an early offer, the Early Offer and End to End RSVP features are mutually exclusive on the SIP Profile Configuration window. When you choose End to End from the RSVP Over SIP drop-down list, the Early Offer support for voice and video calls drop-down list is disabled.<br><br>The Media Transfer Point (MTP) Required check box on the Trunk Configuration window, if enabled, overrides the early offer configuration on the associated SIP profile. Cisco Unified Communications Manager sends the MTP IP address and port with a single codec in the Session Description Protocol (SDP) in the initial INVITE.<br><br>From the drop-down list, select one of the following three options:<br><br>• Disabled (Default value)—Disable Early Offer; no SDP will be included in the initial INVITE for outbound calls.<br><br>• Best Effort (no MTP inserted)<br><br>  • Provide Early Offer for the outbound call only when the caller side media port, IP and codec information are available.<br><br>  • Provide Delayed Offer for the outbound call when caller side's media port, IP address, and codec information is not available. No MTP is inserted to provide Early Offer in this case.<br><br>• Mandatory (insert MTP if needed)—Provide Early Offer for all outbound calls and insert MTP when caller side's media port, IP and codec information is not available. |

The following fields have been changed for the SIP Best Effort Early Offer feature.

| Field | Description |
| --- | --- |
| Send send-receive SDP in mid-call INVITE | Check this check box to prevent Cisco Unified Communications Manager from sending an INVITE a=inactive SDP message during call hold or media break during supplementary services.<br>**Note** This check box applies only to Early Offer or Best Effort Early Offer-enabled SIP trunks and has no impact on SIP line calls.<br>When a SIP INVITE message with a=inactive, sendonly, or recvonly in the audio media line is received on a SIP trunk and sent on a tandem SIP trunk with this check box and either form of Early Offer enabled, Cisco Unified Communications Manager inserts an MTP to provide an SDP with a=sendrcv in the SIP INVITE message that is sent on the tandem SIP trunk. Cisco Unified Communications Manager depends on the SIP devices to initiate reestablishment of the media path by sending either a delayed INVITE or mid-call INVITE with send-recv SDP.<br>When you enable both **Send send-receive SDP in mid-call INVITE** and **Require SDP Inactive Exchange for Mid-Call Media Change** on the same SIP profile, the **Send send-receive SDP in Mid-Call INVITE** setting overrides the **Require SDP Inactive Exchange for Mid-Call Media Change** setting. For SIP line-side calls, the **Send send-receive SDP in mid-call INVITE** check box is not applicable; the **Require SDP Inactive Exchange for Mid-Call Media Change** check box applies when enabled.<br>**Note** To prevent the SDP mode from being set to Inactive in a multiple-hold scenario, set the Duplex Streaming Enabled clusterwide service parameter (**System** > **Service Parameters, Cisco CallManager**) to True. |

| Field | Description |
|---|---|
| Require SDP Inactive Exchange for Mid-Call Media Change | This feature designates how Cisco Unified Communications Manager handles mid-call updates to codecs or connection information such as IP address or port numbers.<br>If the box is checked, during mid-call codec or connection updates Cisco Unified Communications Manager sends an INVITE a=inactive SDP message to the endpoint to break the media exchange. This is required if an endpoint cannot react to changes in the codec or connection information without disconnecting the media. This applies only to audio and video streams within SIP-SIP calls.<br>**Note** For Early Offer or Best Effort early offer-enabled SIP trunks, this parameter will be overridden by the Send send-receive SDP in mid-call INVITE parameter.<br>If the box is unchecked, Cisco Unified Communications Manager passes the mid-call SDP to the peer leg without sending a prior Inactive SDP to break the media exchange. This is the default behavior. |

# Daylight Saving Time Rules

Unified Communications Manager supports daylight savings time (DST) changes for a time zone. DST rules describe DST start and end dates for a time zone annually.

The Unified Communications Manager server generates a new DST rules file every year with DST start and end time for all countries in accordance with the calender year.

The following conditions apply for DST rules file generation:

- A DST rules file is generated for the current year at 00:00 hours on January 10 if the Cisco Unified Communications Manager server is powered on.
- If the Cisco Unified Communications Manager server is not powered on, the DST rules file is generated when the servers boot up, on or after January 10.
- Administrators can generate the DST rules file manually by executing the command **utils update dst** from the command-line interface.

# DST-CiscoSyslog Messages

The following table describes CiscoSyslog messages for DST.

| CiscoSyslog message | Description | Process | Resolution |
|---|---|---|---|
| DST rules file for the current year is created from the cron job.<br>Restart the phones. Not restarting the phones will result in wrong DST start and stop dates. | This message is displayed if the cron job generates the DST rules file successfully. | Cron Job | Ensure phones are restarted after the file is generated. |
| An attempt was made to create the DST rules file from the cron job.<br>DST rules file already created for current year. | This message is displayed if the cron job attempts to generate a new DST rules file even when the file for the current year is already generated. | Cron Job | |
| Cron job failed to create the DST rules file for the current year.<br>Execute **'utils update dst'** to create the DST rules file. | This message is displayed if the cron job fails to generate the DST rules file successfully. | Cron Job | Enter the **utils update dst** from CLI to create the DST rules file. |
| The DST rules file for the current year is created during server reboot.<br>Restart the phones. Not restarting the phones will result in wrong DST start and stop dates. | This message is displayed if server reboot generates the DST rules file successfully. | Bootup Script | Ensure that phones are restarted after the file is generated. |
| An attempt was made to create the DST rules file during server reboot.<br>DST rules file already created for current year. | This message is displayed if server reboot attempts to generate a new DST rules file even when the file for the current year is already generated. | Bootup Script | |
| Server reboot failed to create DST rules file for the current year.<br>Execute **'utils update dst'** to create the DST rules file. | This message is displayed if server reboot fails to generate the new DST rules file successfully. | Bootup Script | Enter the **utils update dst** from CLI to create the DST rules file. |

| CiscoSyslog message | Description | Process | Resolution |
|---|---|---|---|
| DST rules file for the current year is created from CLI.<br>Restart the phones. Not restarting the phones will result in wrong DST start and stop dates. | This message is displayed if the CLI generates the DST rules file successfully. | CLI | Ensure that phones are restarted after the file is generated. |
| An attempt was made to create DST rules file from CLI.<br>DST rules file already created for the current year. | This message is displayed if the CLI attempts to generate a new DST rules file even when the file for the current year is already generated. | CLI | |
| CLI failed to create DST rules file for the current year. | This message is displayed if the CLI fails to generate the new DST rules file successfully. | CLI | |

# utils update dst

This command updates the daylight saving time (DST) rules for the current year.

**utils update dst**

**Command Modes**

Administrator (admin:)

**Usage Guidelines**

This command takes a backup of the existing DST rules file and creates a new DST rules file for the current year.

**Caution** Restart the phones after you execute the command. Not restarting the phones results in wrong DST start and stop dates.

### Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to Unified Communications Manager and IM and Presence service.

# Directory Search in Self Care

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

# Embedded Cisco TelePresence Management Suite in Self Care Portal

You can configure Unified Communications Manager to open the Cisco TelePresence Management Suite (TMS) User Portal within the Conferencing tab of the Self Care Portal.

With this configuration, when users who are configured with TelePresence select the **Conferencing** tab and then select **Schedule a Meeting**, the TMS User Portal opens inside the application interface rather than in a separate popup window.

## Enable Embedded TelePresence for Self Care Portal

Follow this procedure to embed the TMS User Portal into the Self Care Portal interface.

### Before You Begin

- Configure a Video Conference Server UC Service and a Service Profile with the Video Conferencing UC Server.
- Associate the Service Profile to the end users who will use Self Care.

### Procedure

**Step 1** From Cisco Unified CM Administration, select **System** > **Enterprise Parameters**.

**Step 2** Navigate to **Self Care Portal Parameters**.

**Step 3** From the **Show Video Conference Scheduler** drop-down list, select **Show in Conferencing tab**.

**Note** If the TMS User Portal does not appear properly in the Self Care Portal, the browser may not support this function. In this case, select **Show as Browser Popup**.

The Cisco TelePresence Management Suite conferencing status will appear in the Self Care Portal window for the end user.

# IM and Presence Service Deprecation of Microsoft Exchange Server 2003

Microsoft Exchange Server 2003 is no longer supported for Cisco Unified Communications Manager IM and Presence Service, Release 10.5 and later.

# IM and Presence Service Deprecation of WebDAV

WebDAV is being deprecated from Release 10.5 and later. All clients with WebDAV configured integrations must remove WebDAV or switch to EWS before upgrading to 10.5.

# IM and Presence Service IPv6 Support

IM and Presence Service supports Internet Protocol version 6 (IPv6), which uses packets to exchange data, voice, and video traffic over digital networks. IPv6 also increases the number of network address bits from 32 bits in IPv4 to 128 bits. IPv6 deployment in the IM and Presence Service network functions transparently in a dual-stack IPv4 and IPv6 environment. The default network setting is IPv4.

Outbound IPv6 traffic is allowed when IPv6 is enabled. For example, SIP S2S can be configured to use either static routes or DNS queries. When a static route is configured and IPv6 is enabled, the SIP proxy attempts to establish an IPv6 connection if IPv6 IP traffic is provided. You can use IPv6 for connections to external databases, LDAP and Exchange servers, and for federation connections on IM and Presence Service even though the connection between IM and Presence Service and Cisco Unified Communications Manager uses IPv4.

If the service uses DNS requests (for example, with XMPP S2S), then after receiving the list of IP addresses as the result of the DNS query, the service attempts to connect to each IP address on the list one by one. If a listed IP address is IPv6, the server establishes an IPv6 connection. If the request to establish the IPv6 connection fails, the service moves on to the next IP address on the list.

If for any reason IPv6 gets disabled for either the enterprise parameter or for ETH0 on the IM and Presence Service node, the node can still perform internal DNS queries and connect to the external LDAP or database server if the server hostname that is configured on IM and Presence Service is a resolvable IPv6 address.

For additional information about IPv6 and for network guidelines, see the following documents:

- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager Features and Services Guide*
- *Command Line Interface Guide for Cisco Unified Communications Solutions*
- *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager*
- *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*

## IPv6 Configuration

To enable IPv6 for IM and Presence Service, you must perform the following tasks:

- Configure IPv6 on Eth0 for each IM and Presence Service node in the cluster using either the Cisco Unified IM and Presence OS Administration GUI or the Command Line Interface.
- Enable the IPv6 enterprise parameter for the IM and Presence Service cluster.

You must configure IPv6 for both the IM and Presence Service enterprise network and for Eth0 on each IM and Presence Service node for IPv6 to be used; otherwise, the system attempts to use IPv4 for IP traffic. For example, if the enterprise parameter is set to IPv6 and only one of two nodes in the cluster has their Eth0 port set for IPv6, then only the node with the port set to IPv6 is enabled for IPv6. The other node will attempt to use IPv4.

For configuration changes to the IPv6 enterprise parameter to take affect, you must restart the following services on IM and Presence Service:

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router

For instructions to configure IPv6 for IM and Presence Service, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

For more information about using the Command Line Interface to configure IPv6 parameters, see the *Cisco Unified Communications Manager Administration Guide* and the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

# IPv6 Interactions and Restrictions

Observe the following interactions and restrictions when configuring IPv6 on IM and Presence Service and when interacting with external IPv6 devices and networks:

- You can use IPv6 for your external interfaces on IM and Presence Service even though the connection between IM and Presence Service and Cisco Unified Communications Manager uses IPv4.
- You must configure IPv6 for the IM and Presence Service enterprise network and for Eth0 on each IM and Presence Service node to use IPv6; otherwise, the system attempts to use IPv4 for IP traffic on the external interfaces. For example, if the enterprise parameter is set to IPv6 and only one of two nodes in the cluster has their Eth0 port set for IPv6, then only the node with the port set to IPv6 is enabled for IPv6. The other node will attempt to use IPv4.

**Note** If for any reason IPv6 gets disabled for either the enterprise parameter or for ETH0 on the IM and Presence Service node, the node can still perform internal DNS queries and connect to the external LDAP or database server if the server hostname that is configured on IM and Presence Service is a resolvable IPv6 address.

- For federation, you must enable IM and Presence Service for IPv6 if you need to support federated links to a foreign Enterprise that is IPv6 enabled. This is true even if there is an ASA installed between the IM and Presence Service node and the federated Enterprise. The ASA is transparent to the IM and Presence Service node.

- If IPv6 is configured for any of the following items on the IM and Presence Service node, the node will not accept incoming IPv4 packets and will not automatically revert to using IPv4. To use IPv4, you must ensure that the following items are configured for IPv4 if they appear in your deployment:
  - Connection to an external database.
  - Connection to an LDAP server.
  - Connection to an Exchange server.
  - Federation deployments.

# New CLI Commands

## set network ipv6 dhcp

This command sets the DHCPv6 client on the server and enables IPv6 support. For changes to take effect, you must restart the server.

**set network ipv6 dhcp** {**enable**| **disable**} **[reboot]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **dhcp** | Sets the DHCPv6 client on the server. By default, the server does not restart after you enable the DHCPv6 client. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| **enable** | Enables IPv6 support. |
| **disable** | Disables IPv6 support. |
| **reboot** | (Optional) Causes the server to automatically restart after you enter the command. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

## set network ipv6 gateway

This command sets the IPv6 gateway for the server. For changes to take effect, you must restart the server.

**set network ipv6 gateway** *addr* **[reboot]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **gateway** | Sets the IPv6 gateway for the server. By default, the server does not restart after you set the IPv6 gateway for the server. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| *addr* | The IPv6 gateway address. |
| **reboot** | (Optional) Causes the server to automatically restart after you enter the command. |

**Command Modes**

Administrator (admin:)

**Requirements**

Command privilege level: 1

Allowed during upgrade: No

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

## set network ipv6 service

This command enables or disables the IPv6 service on the server. For changes to take effect, you must restart the server.

**set network ipv6 service** {**enable**| **disable**} **[reboot]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **service** | Sets the IPv6 service on the server. By default, the server does not restart after you enable or disable the IPv6 service on the server. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| *enable* | Enables IPv6 service on the server. |
| *disable* | Disables IPv6 service on the server. |
| **reboot** | (Optional) Causes the server to automatically restart after you enter the command. |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

## set network ipv6 static_address

This command assigns the static IPv6 address to the server. For changes to take effect, you must restart the server.

**set network ipv6 static_address** *addr mask* **[reboot]**

**Syntax Description**

| Parameters | Description |
|---|---|
| **static_address** | Assigns a static IPv6 address to the server. By default, the server does not restart after you assign the static IPv6 address. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| *addr* | Specifies the static IPv6 address you assign to the server. |
| *mask* | Specifies the IPv6 network mask (0-128). |
| **reboot** | (Optional) Causes the server to automatically restart after you enter the command. |

**Command Modes**

Administrator (admin:)

### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

# IM and Presence Service Support for Encrypted External Database

### User Interface

In the **Cisco Unified CM IM and Presence Administration** user interface, under **Messaging** > **External Server Setup** > **External Databases**, an Enable SSL check box and a Certificate Name drop-down list have

been added to the External Database Settings area. These become active when you choose Oracle as the Database Type.

### Certificates

- When the SSL field or the Certificate drop-down field is modified, a notification to restart the corresponding service assigned to the external database is sent. A message concerning either "Cisco XCP Message Archiver" or "Cisco XCP Text Conference Manager" will be generated.
- The certificate you need to enable SSL must be uploaded to the cup-xmpp-trust store.
- Once the certificate is uploaded to the cup-xmpp-trust store, you must wait 15 minutes for the certificate to propagate to all the nodes of the IM and Presence Service cluster. If you do not wait, the SSL connection on nodes where the certificate has not propagated fails.

### System Troubleshooter

In the **Cisco Unified CM IM and Presence Administration** user interface, the results of a troubleshooting test has been made more descriptive. The test results are shown in the **System Configuration Troubleshooter** window, External Database Troubleshooter area (under **Diagnostics** > **System Troubleshooter**). The test result is also shown in the **External Database Settings** window, External Database Status area (under **Messaging** > **External Server Setup** > **External Databases**) .

The test is:

- Verify external database server connectivity (database connection check)

### Real Time Monitoring Tool (RTMT)

If the certificate is missing or has been deleted from the cup-xmpp-trust store, an alarm 'XCPExternalDatabaseCertificateNotFound' is raised in the Cisco Unified Communications Manager RTMT.

# Support Variable Extension Length and +E.164 for LDAP Directory Numbers

### Cisco Unified Communications Administrator Guide Updates

In Cisco Unified Communications Manager, use the **System** > **LDAP** > **LDAP Directory** menu path to configure LDAP directories. The following changes are applicable to the following fields in LDAP directory settings:

| Field | Description |
|---|---|
| Apply mask to synced telephone numbers to create a new line for inserted users | Check the check box to apply mask to the synced telephone number of the user.<br>Enter a mask value in the **Mask** text box.<br>**Note**<br>• The mask must contain numbers (0-9), X, and x. It must include at least one x or X.<br>• The mask can have + or \+ special characters only at the start position.<br>• The applied mask length is the same as the entered telephone number, even if the number of characters that are entered for the mask is longer than the telephone number.<br>• If the mask is longer then, it is applied from right to left of the entered telephone number.<br>For example, if you set the mask as 11XX for the user with a telephone number 8889945, after the mask is applied, 1145 becomes the primary extension of the user. |
| Assign new line from the pool list if one was not created based on a synced LDAP telephone number | Check the check box to assign a new line from the DN pool list. |
| Next Candidate DN | Displays the next probable DN that will be assigned to the user.<br>The DN from the next DN pool is displayed only after all the DNs from the first DN pool are assigned.<br>**Note** The **Next Candidate DN** is displayed only when you check the **Assign new line from the pool list if one was not created based on a synced LDAP telephone number** check box. |

| Field | Description |
|---|---|
| Add DN Pool | By default, only one DN pool is available. Click this option to add more DNs to the DN pool.<br>Enter the **DN Pool Start** and **DN Pool End** values in the text box.<br>You can reorder the DN pool to prioritize the DNs that you want to assign. The DN pool values must conform to the following requirements:<br>• **DN Pool Start** and **DN Pool End** must be numbers only.<br>• DN length in **DN Pool Start** and **DN Pool End** must be identical with a maximum length of 20 characters excluding + or \+.<br>• **DN Pool Start** and **DN Pool End** can have + or \+ special characters only at the start position.<br>• **DN Pool End** must be greater than **DN Pool Start**,<br>• **DN Pool Start** and **DN Pool End** must not be null,<br>• DN range is between 0 to 10,000,000.<br>You can create only three DN pools. |

# Voice Gateway Support

The following gateways are supported by Cisco Unified Communications Manager release 10.0 - 10.5. For this release, documentation has been added.

- Cisco Integrated Services Router 4451-X
- Cisco VG310 Analog Phone Gateway
- Cisco VG320 Analog Phone Gateway
- Cisco VG350 Analog Phone Gateway

The following sections summarize gateway support in Cisco Unified Communications Manager.

## Cisco Voice Gateways (ISR) 44XX Series

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

- T1 CAS/PRI and E1/PRI signaling using MGCP

- T1/PRI and PRI using SIP or H.323

## Cisco ISR44XX Series Gateways

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

The key features of the gateways are:

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

### Cisco Integrated Services Router 4451-X

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

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

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

## Cisco Voice Gateways

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

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

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

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

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

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

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

- FXS

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

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

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

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

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

### Standalone Voice Gateways

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

#### *Cisco VG310 Analog Phone Gateway*

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

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

#### *Cisco VG320 Analog Phone Gateway*

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

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

#### *Cisco VG350 Analog Phone Gateway*

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

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

## Voice Gateway Model Summary

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

***Table 27: Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Port Types***

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

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

# New CLI Commands

### Related Topics

utils update dst, on page 38

## utils vmtools refresh

This command refreshes the currently installed VMware Tools to the latest version that is prescribed by the ESXi host for that VM.

**utils vmtools refresh**

### Command Modes

Administrator (admin:)

### Usage Guidelines

To update the current version of the VMware Tools, select **Guest** > **Install/Upgrade VMWare Tools** > **Interactive Tools Upgrade**.

#### Requirements

Command privilege level: 1

Allowed during upgrade: No

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

#### Example

```
admin:utils vmtools refresh
VMware Tools match host. Upgrade allowed, though not required.
```

```
***   W A R N I N G   ***
Running this command will update your current version of VMware Tools
to the latest version prescribed by the ESXi host on which this VM is
running. The tools install will cause your system to reboot twice.
```

# Windows 8.1 and Windows Server 2012 R2 Support

With Cisco Unified Communications Manager Release 10.5(1), the following client applications support Windows 8.1 (32-bit and 64-bit) operating system and Windows Server 2012 R2 operating system:

- Cisco Unified TAPI Client
- Cisco Unified JTAPI Client
- Cisco Unified Real-time Monitoring Tool (RTMT)
- Cisco Unified Communications Manager Cisco Trust List (CTL) Client
- Cisco Unified Communications Manager Assistant Console

**Note** Windows User Account Control (UAC) must be disabled to run Cisco Unified CM Assistance Console on Windows 8.x.

# About Cross-Origin Resource Sharing

Cross-Origin Resource Sharing (CORS) is a function that allows JavaScript on a web page of one domain to make XMLHttpRequests to another domain. Such cross-domain requests would otherwise be forbidden by web browsers, based on the security policy. CORS defines a way in which the browser and Unified Communications Manager can interact using the User Data Service (UDS) interface to determine whether or not to allow the cross-origin request. This provides a method that is more useful than only allowing same-origin requests, and is more secure than only allowing all of these cross-origin requests.

CORS is particularly useful for web-based applications that use the UDS interface on Unified Communications Manager and the Unified Messaging interface (CUMI) on Cisco Unity Connection.

For example: A web application provides an end user with capabilities to manage their voice settings. This web application is hosted at https://domaina/webapps/vsettings.html and requires access to UDS, which is hosted on Unified Communications Manager servers. Due to cross-domain restrictions, the web application normally would be denied access to UDS because the web application and UDS are from different domains. With CORS, the system administrator using Unified Communications Manager Administration can give permission to applications that are hosted at https://domaina to access UDS.

CORS is also useful for developers who are integrating Jabber SDK and Unified Communications Manager directory services with web-based applications such as those that are provided by cloud services that are hosted in different domains. For example, a cloud service integration that needs to look up Unified Communications Manager contact information for people in an instant-messaging contact list would benefit from CORS in situations where the Unified Communications Manager domain differs from that of the cloud service.

When CORS is configured, Unified Communications Manager allows cross-domain requests like Get User or Put Credentials to succeed. When CORS is not configured, Unified Communications Manager rejects cross-domain requests.

# Configure Cross-Origin Resource Sharing

### Procedure

**Step 1** In Cisco Unified Communications Manager Administration, choose **System** > **Cross-Resource Sharing (CORS)**.
The Find and List Cross-Resource Sharing (CORS) web page.

**Step 2** Set the Preflight Response Cache Settings. The settings allow you to customize the amount of time that you want the verification information to remain live in the browser's cache.

**Step 3** To add a domain to access User Data Service (UDS), click **Add New**.

**Step 4** Enter the domain in the **Domain** field.
The protocol must be defined and wildcards are permitted as a standalone entry or after the protocol. For example: http://*.mycompanyinternalsite.com.

**Step 5** Enter a description in the **description** field.

**Step 6** Choose an access level. These access levels are intended to restrict the HTTP Methods that are allowed by UDS.

- Read-Only — Allows only the Get and Head methods, which are for obtaining information and not for changing it.
- Full-Access — Allows for Read-Only and adds the Post, Put, and Delete methods. If you intend your web applications to support full CRUD (Create, Read, Update, and Delete) operations, Full-Access.

**Step 7** Click **Save**.

# Configure LDAP Directory

Cisco Unified Communications Manager supports user synchronization and authentication with the following LDAP directories:

- 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

### Real-Time Measuring Tool Performance Counters for LDAP Directory

Cisco Unified Communications Manager Release 10.5 adds two new Real-Time Measuring Tool (RTMT) performance counters for LDAP Directory to help Administrators monitor account synchronization status.

**Performance Counters**

- Accounts Failed – The number of user accounts that failed to synchronize during the last directory synchronization operation.
- Accounts Synchronized – The number of user accounts successfully synchronized during the last directory synchronization operation.

# New RTMT Alert for Global Dial Plan Replication

The following Cisco Unified Real-Time Monitoring Tool alert has been added for Global Dial Plan Replication feature:

**ILSDuplicateURI**

This alert occurs when the Cisco Unified Communications Manager identifies that it has learned duplicate Universal Resource Identifier (URI) entries through Intercluster Lookup Service (ILS) during a call to the URI. Whenever there are duplicate entries for a URI, such as the URI user@example.com existing on two clusters, the call is always routed to the cluster from which the URI was first learned. Calls are not routed to the other duplicate entries.

**Default Configuration**

| Value | Default Configuration |
|---|---|
| Enable Alert | Selected |
| Severity | Alert |
| Enable/Disable this alert on the following servers | Enabled on listed servers |
| Threshold | Trigger alert when the following condition is met:<br>Duplicate URI is found in the remote cluster |
| Duration | Trigger alert immediately |
| Frequency | Trigger alert on every poll |
| Schedule | Trigger alert when it occurs |
| Enable Email | Selected |
| Trigger Alert Action | Default |

# Silent Monitoring CLI Update

With release 10.5(1), Cisco Unified Communications Manager now supports the `set replication-sync monitor` CLI command for silent monitoring. This CLI command turns on the replication monitoring service. This command replaces the `set replwatcher monitor` CLI command from previous releases, which is no longer supported.

## Set replication-sync monitor

This command enables or disables replication monitoring by the Cisco Replication Watcher service. The Cisco Replication Watcher service blocks other services from starting until database replication is setup and functioning normally.

**set replication-sync monitor {enable | disable}**

### Syntax Description

| Parameters | Description |
|---|---|
| **enable** | Turns on the replication monitoring service. |
| **disable** | Turns off the replication monitoring service |

### Command Modes

Administrator (admin:)

#### Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: IM and Presence service on Unified Communications Manager only

# Product-Specific Configuration in TelePresence Device User Interfaces

With this feature, users can set their product-specific configuration from certain Cisco TelePresence device interfaces. The information that the user enters is then sent to Unified Communications Manager so that the device settings are synchronized.

# Cisco IP Phones and Cisco Desktop Collaboration Experience DX650

## Cisco IP Phones

### Cisco IP Phone Firmware Versions

The following table lists the latest Cisco IP Phone firmware version supported for Cisco Unified Communications Manager 10.5.

***Table 28: Phone Firmware Versions***

| Phone family | Firmware release number |
|---|---|
| Cisco Unified SIP Phone 3905 | 9.4(1) |
| Cisco Unified IP Phones 6901 and 6911 | 9.3(1)SR1 |
| Cisco Unified IP Phones 6921, 6941, 6945, and 6961 | 9.4(1)SR1 |
| Cisco IP Phone 7800 Series | 10.1(1)SR1 |
| Cisco Unified IP Phone 7900 Series | 9.3(1)SR4 |
| Cisco Unified Wireless IP Phone 792x Series | 1.4(5) |
| Cisco Unified IP Conference Phone 8831 | 9.3(3) |
| Cisco Unified IP Phones 8941 and 8945 | 9.4(1)SR1 |
| Cisco Unified IP Phones 8961, 9951, and 9971 | 9.4(1)SR1 |

### Cisco Unified SIP Phone 3905 Features

No features have been introduced to the Cisco Unified SIP Phone 3905.

### Cisco Unified IP Phone 6900 Series Features

No features have been introduced to the Cisco Unified IP Phone 6901 and 6911.

The following table lists the features added to the Cisco Unified IP Phone 6921, 6941, 6945, and 6961 for firmware release 9.4(1)SR1. For more information, see the Release Notes at the following location:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-6900-series/products-release-notes-list.html

| Feature name | Firmware release |
|---|---|
| Rate Limit for Multicast and Broadcast Traffic | 9.4(1)SR1 |

## Cisco IP Phone 7800 Series Features

The following table lists the features added to the Cisco IP Phone 7800 Series for firmware release 10.1(1)SR1. For more information, see the Release Notes at the following location:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-release-notes-list.html

| Feature name | Firmware release |
|---|---|
| Hardware Updates | 10.1(1)SR1 |

## Cisco Unified IP Phone 7900 Series Features

The following table lists the features added to the Cisco Unified IP Phone 7900 Series for firmware release 9.3(1)SR4. No new features were added for firmware release 9.3(1)SR3. For more information, see the Release Notes at the following location:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-release-notes-list.html

| Feature name | Firmware release |
|---|---|
| Control Default Wallpaper | 9.3(1)SR4 |
| Default Audio Path Support | 9.3(1)SR4 |
| DSP Audio Enhancement Support | 9.3(1)SR4 |
| Hardware Updates | 9.3(1)SR4 |

## Cisco Unified Wireless IP Phone 792x Series Features

No features have been introduced to the Cisco Unified Wireless IP Phone 792x Series.

## Cisco Unified IP Conference Phone 8831 Features

No features have been introduced to the Cisco Unified IP Conference Phone 8831.

## Cisco Unified IP Phones 8941 and 8945 Features

The following table lists the features added to the Cisco Unified IP Phones 8941 and 8945 for firmware releases 9.3(4) and 9.4(1). No new features were introduced for firmware release 9.4(1)SR1. For more information, see the Release Notes at the following location:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8900-series/products-release-notes-list.html

| Feature name | Firmware release |
|---|---|
| Adaptive Bandwidth Management | 9.4(1) |
| Bandwidth Management Enhancement | 9.3(4) |
| Configurable Volume Autosave | 9.4(1) |
| Electronic Hookswitch | 9.4(1) |
| E-SRST Service Improvements | 9.3(4) |
| Flexible DSCP Marking | 9.4(1) |
| Gateway Recording for SIP | 9.4(1) |
| Hold or Resume Toggle from Hard Key | 9.3(4) |
| Larger Font for Time and Date | 9.3(4) |
| Minimum Ring Volume | 9.3(4) |
| Peer Firmware Sharing | 9.4(1) |
| Remotely Check CTL and ITL File | 9.3(4) |
| Report CTL and ITL Information | 9.3(4) |
| Ringtone and Wallpaper Customization API | 9.4(1) |
| RTCP Always On | 9.4(1) |
| Secondary Load Server | 9.3(4) |
| Serviceability for SIP Endpoints | 9.4(1) |
| Video Through PC | 9.3(4) |
| Video UI Enhancement | 9.3(4) |
| Visual Voicemail | 9.3(4) |

| Feature name | Firmware release |
|---|---|
| W360p By Default | 9.3(4) |

### Cisco Unified IP Phones 8961, 9951, and 9971 Features

No features have been introduced to the Cisco Unified IP Phones 8961, 9951, and 9971.

## Cisco DX Series

### Cisco DX650 Firmware Versions

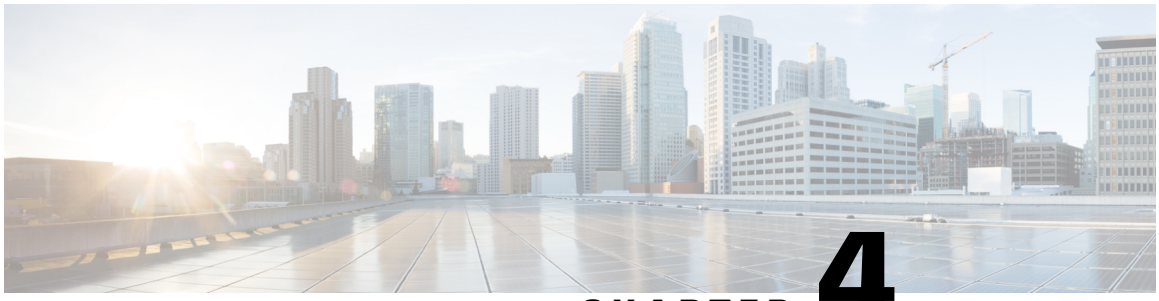
The following table lists the latest Cisco DX650 firmware version supported for Cisco Unified Communications Manager 10.5.

| Device | Firmware Release Number |
|---|---|
| Cisco DX650 | 10.1(2)SR1 |

#### Cisco DX650 Features

The following table lists the features added to the Cisco DX650 for firmware release 10.1(2). For more information on the Cisco DX650, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-release-notes-list.html

| Feature name | Firmware release |
|---|---|
| Public Mode | 10.1(2) |
| Video Greetings | 10.1(2) |



CHAPTER 4

# Important Notes


- Call Control, page 61
- Installation, page 62
- Disaster Recovery System, page 62
- Features and Services, page 63
- IM and Presence Service, page 64
- Interoperability, page 65
- Miscellaneous, page 66


# Call Control

## Conference Call Video Problem

This information applies to CSCup01790.

Cisco Unified Communications Manager allocates an audio only conference bridge when the initial leg is triggered from an audio capable phone to video capable phones through an Early Offer (EO) or Best Effort Early Offer (BEEO) trunk. This scenario disables video in a conference call, even when video-capable endpoints are connected. To avoid this problem, you must perform the following steps.

### Procedure

**Step 1** Set the **Allocate Video Conference Bridge For Audio Only Conferences When The Video Conference Bridge Has Higher Priority** service parameter to **True**.

**Step 2** In the MRGL list, set the video conference bridge with a higher priority than the audio conference bridge.

## 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.

# 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.

# 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

## 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)`

## IM and Presence Service Needs to Support Install Against a Small Disk Cisco Unified Communications Manager Publisher

This information applies to CSCuo54588

Cisco Unified Communications Manager IM and Presence Service cannot be deployed when a Cisco Unified Communications Manager 40-GB- or 60-GB-disk OVA deployment size is used.

The IM and Presence Service installer determines whether the publisher node is a valid system. The installer interprets a Cisco Unified Communications Manager OVA deployment size of less than 80 GB (for example, 40 GB or 60 GB) as invalid and does not proceed with the installation.

The only way to resolve this issue is to use a Cisco Unified Communications Manager OVA deployment option that utilizes the full-size 80-GB disk at a minimum. For more information about supported OVA deployment options, see http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CM_IM_and_Presence.

# 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.

## 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.

# Miscellaneous

## 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.

## 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
```

## 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.

## Presence Web Service Unable to Send Event Notification if Endpoint Registered with FQDN

This information applies to CSCuo48936.

If a Presence Web Service (PWS) application registers an endpoint using anything other than an IP address, the PWS is unable to send notifications to that endpoint. As a result, applications that were developed using the PWS are unable to receive events from IM and Presence Service nodes. To resolve this issue, you must use an IP address when registering the endpoint.

# 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.

# 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.

# SIP Trunk Not Properly Reset until CFB is Reset

This information applies to CSCup05922.

The following behavior is observed in SIP trunks for Cisco Unified Communications Manager Release 10.5(1):

**Note** When you check the **Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"** check box, you must reset or restart all of the associated devices. The changes in the status of SIP trunks are reflected on the **Trunk Find List** window with a time delay of 5 minutes.

# Devices Reset with Certificate Regeneration

This information applies to CSCus63274.

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

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

This information applies to CSCut08346.

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

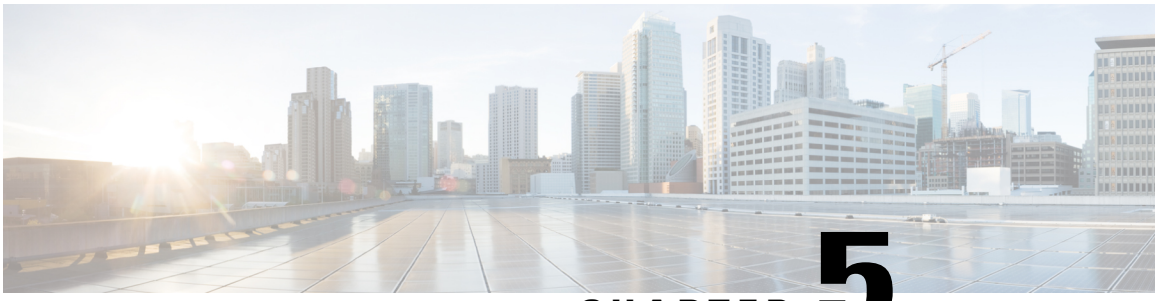
# Perfect Forward Secrecy is not Supported in IPsec Configuration

This information applies to CSCuu74346.

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

# Change Perfmon Counter File Size Parameters in RTMT

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



CHAPTER 5

# Documentation Updates


- Administration Guide, page 72
- Bulk Administration Guide, page 83
- Call Detail Records Administration Guide, page 85
- CLI Reference Guide, page 89
- Disaster Recovery System Guide, page 89
- Features and Services Guide, page 90
- JTAPI Developers Guide, page 97
- Managed Services Guide, page 98
- Online Help for Cisco Unified Communications Manager, page 98
- OS Administration Guide, page 99
- Real-Time Monitoring Tool Guide, page 100
- Security Guide, page 101
- Serviceability Guide, page 106
- System Guide, page 109
- TAPI Developers Guide, page 112
- TCP and UDP Port Usage Guide, page 112
- Upgrade Guide, page 113
- Configuration and Administration Guide for IM and Presence Service, page 114
- Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service, page 114

# 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.<br>For Cisco VG248 gateways, begin the description with`VGC<mac address>`.<br>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*.<br><br>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.<br><br>**Tip** Remember to update the DNS server with the appropriate Cisco Unified Communications Manager name and address information.<br><br>**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 29: 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*.<br>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 30: 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.<br>**Note** This field is mandatory. |

# 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.<br>This is the pattern to which the original call was placed before any configured translation rules are applied.<br>Default—empty string "". |
| finalCalledPartyPattern | Text String | Numeric string (with special characters) string up to 50 characters.<br>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.<br>This value is the same as the finalCalledPartyNumber if the number is a direct match without any translation<br>Default—empty string "". |

| Field Name | Range of Values | Description |
|---|---|---|
| lastRedirectingPartyPattern | Text String | Numeric string (with special characters) string up to 50 characters.<br>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.<br>Default—empty string "". |
| huntPilotPattern | Text String | Numeric string (with special characters) string up to 50 characters.<br>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.<br>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 |
| lastRedirectDn | 136111 | 136203 | 136201 | 136201 | 136201 | 136203 |
| origCause_Value | 393216 | 0 | 16 | 393216 | 393216 | 0 |
| dest_CauseValue | 393216 | 0 | 393216 | 393216 | 393216 | 16 |
| **authCodeDescription** | | Forward_FAC | | | | |
| **authorizationLevel** | 0 | 1 | 0 | 0 | 0 | 0 |
| Duration | 18 | 0 | 37 | 37 | 32 | 38 |
| authorizationCode | | 124 | | | | |

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

### CMC Example 2

Blind conference using CMC :

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

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

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

# CLI Reference Guide

## ILS Troubleshooting Tips Corrections

This documentation update resolves CSCun09203.

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

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

**utils ils find route** is an invalid command.

## Show perf query counter Command Output

This documentation update resolves CSCuo70238.

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

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

## 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 31: 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.<br>Version compatibility depends on your version of Unified Communications Manager and Cisco Prime Collaboration Deployment. See the *Cisco Prime Collaboration Deployment Admin Guide* before you upgrade its version (SFTP) or Unified Communications Manager to ensure that the versions are compatible. |
| SFTP Server from a Technology Partner | These servers are third party provided, third party tested, and jointly supported by TAC and the Cisco vendor.<br>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:<br>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.<br>Version compatibility is on a best effort basis to establish compatible SFTP versions and Unified Communications Manager versions.<br>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 32: Cisco Unified IP Phones That Use iDivert or Divert Softkeys***

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

# 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 33: Default Configuration for the LogPartitionLowWaterMarkExceeded RTMT Alert***

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

## Incorrect Minimum Rate for Monitoring a Performance Counter

This documentation update resolves CSCuz11160.

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

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

## LowAvailableVirtualMemory Threshold Value is Incorrect

This documentation update resolves CSCuu72197.

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

## 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:<br>• Cluster ID is unique across all the hub nodes in the ILS cluster.<br>• Fully Qualified Domain Name (FQDN) is configured.<br>• UDS and EM services are running on the all of the hub nodes in the ILS cluster.<br>• DNS primary and reverse resolution are working fine.<br>• Import consolidated Tomcat certificates from all the hub nodes.<br>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

## 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.

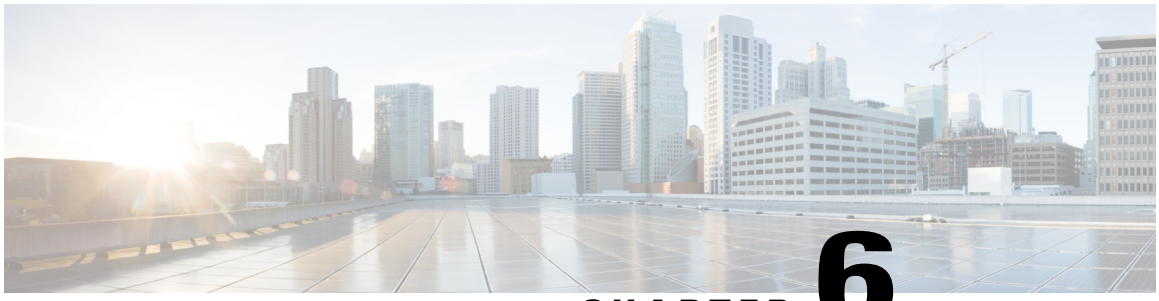
**Step 3** Click **Yes** to reboot the system.
The new domain name gets updated after the system is rebooted

**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*.



CHAPTER 6

# Caveats


- Bug Fixes and Updates, page 117
- Bug Search Tool, page 117
- Resolved Caveats, page 118
- Open Caveats, page 118


## Bug Fixes and Updates

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

## Bug Search Tool

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

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

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

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

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

Follow these steps to use Cisco Bug Search tool:

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

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

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

# Resolved Caveats

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

**Tip**

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

### Related Topics

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

# Open Caveats

## Caveats

## a-Open Caveats for Cisco Unified Communications Manager, Release 10.5(1)

*Table 34: Open Caveats for Unified Communications Manager, Release 10.5(1)*

| Identifier | Severity | Component | Headline |
|---|---|---|---|
| CSCun74694 | 3 | bat | UPD BAT inserts fail when "Override Configuration "options are enabled |
| CSCuo77612 | 3 | bps-bat | BAT user import is resetting the password |

| Identifier | Severity | Component | Headline |
|---|---|---|---|
| CSCum95475 | 3 | car | CUCM CAR Web Application Vulnerable to CSRF Attack |
| CSCui28980 | 3 | ccm-serviceability | Service Restart status is abnormal |
| CSCuo17302 | 3 | ccm-serviceability | CUCM RTMT absolute path traversal file delete |
| CSCuo17199 | 3 | ccm-serviceability | CUCM RTMT absolute path traversal |
| CSCun71682 | 3 | cli | cmdImportConfig uses insecure password encryption |
| CSCuo70122 | 3 | cmcti | CTIport remain to be Out of Service when another app invokes register |
| CSCuo76294 | 3 | cmcti | CTI reports same permanent line ID for ParkDNs starting with non-digit |
| CSCuo74945 | 3 | cmui | Error occurred during find. Column (license count) not found |
| CSCuo61115 | 3 | cmui | Sub CUCM does not show as available for new CUCM Group |
| CSCuo17455 | 3 | cmui | CUCM should escape all text from banner text file |
| CSCuo55881 | 3 | cmui | Dependency issues for Access List Page |
| CSCuo31753 | 3 | cmui | Unified Reporting shows replication is not established |
| CSCuo54416 | 3 | cp-cac | CCM memory leak in mSides map at LBMInterface |
| CSCuo64820 | 3 | cp-callcontrol | CAL level displayed different on phone |
| CSCuo69582 | 3 | cp-callcontrol | Call index is 2 for the only call |
| CSCul81569 | 3 | cp-linecontrol | SDLLinkOOS causes CCM Core - LineManager::wait RemoteLineOOS |
| CSCuo66008 | 2 | cp-mediacontrol | ccm core in AudioCapStructArray::copy Common Data |
| CSCuo79182 | 3 | cp-mediacontrol | SipInterface doesn't send SDPOfferInd with SDP to the Media Exchange |
| CSCuo74745 | 3 | cp-mediacontrol | S2 Escalation 629796265: Hold/Resume on calls from IP phone to PSTN drop |
| CSCuo76752 | 3 | cp-mgcp | CCM core is generated when a very long number is called via MGCP |

| Identifier | Severity | Component | Headline |
|---|---|---|---|
| CSCuo78952 | 3 | cp-sip-station | Single Number Reach voice mail detection (VMA) call cant be answered |
| CSCuo71657 | 3 | cp-sip-station | Transcoder not inserted when phone SIP Phone codec locked for recording |
| CSCuo48985 | 3 | cp-sip-station | Transfer a secure call from SIP secure-device to non-secure phone fails |
| CSCuo77984 | 3 | cp-sip-station | CSCug25138 need to be back ported |
| CSCun74320 | 3 | cpi-appinstall | Overly open permissions on platformConfig.xml |
| CSCuo71306 | 2 | cpi-appinstall | Inbound SIP IPv6 Calls from CUBE over UDP transport exhibit failures |
| CSCuh19734 | 3 | cpi-cert-mgmt | Uploading certs with same CN will overwrite old cert in Phone-VPN-trust |
| CSCum998390 | 3 | cpi-os | Upgrade the Tomcat version to 7.0.52 |
| CSCuo31083 | 3 | cpi-os | Upgrade JDK to 1.7.0_55 |
| CSCun92401 | 3 | cpi-os | RHEL6 Kernel vulnerabilities on VOS Platform |
| CSCuo75130 | 3 | cpi-os | Deprecated pam_stack module called from service “sshd” warnings |
| CSCuo72650 | 3 | cpi-platform-api | Wrong Platform API version after the installation of the UK local file |
| CSCun74385 | 3 | cpi-security | Weak derivation of sftpuser password from cluster security password |
| CSCuo71657 | 3 | cp-sip-station | Transcoder not inserted when SIP phone codec locked for recording |
| CSCun00701 | 3 | cuc-tomcat | CUCM OS Administration Vulnerable to CSRF Attack |
| CSCun74317 | 3 | cuc-tomcat | Potentially unsafe permissions on Tomcat directories |
| CSCuo19778 | 3 | database-ids | PMR 87550: Database clients leak memory after close |
| CSCuo38244 | 3 | gaxl | Low Available Virtual Memory on Publisher after 10.5 upgrade |
| CSCuo58633 | 3 | ils | Route Plan Report shows Unmapped Exception error |

| Identifier | Severity | Component | Headline |
|---|---|---|---|
| CSCuh52778 | 3 | ims | CCMEncryption Uses Poor Random Numbers for Cryptographic Purposes |
| CSCum58598 | 3 | ims | Phone web server does not limit number of failure authentication attempt |
| CSCuo78241 | 3 | ipma-service | Assistant which is not default (current) can change the manager settings |
| CSCuo65649 | 3 | media_str_app | IPVMS core occurred during load run |
| CSCuo76378 | 2 | risdc | RTMT Alerts for services down even though they are up |
| CSCuo76601 | 3 | saml-sso | Certificate exception message displayed after OpenAM SAML/SSO enabled. |
| CSCuo58257 | 3 | security | SSO: tkssmode 0 when AgentFlow SSO enabled during 8.6.1 to 10.5 upgrade |
| CSCuo36200 | 3 | selfcare | CUCM 10.5 - login banner removed/missing |
| CSCuo08984 | 3 | selfcare | Self Care: Hardcoded strings |
| CSCun18651 | 3 | selinux | SELinux denials not logged in messages in CUCM 10.0(1) |
| CSCuo41138 | 3 | tftp | TFTP service crashes generating core dump |
| CSCuo63567 | 3 | ucmap | About 29 seconds for page to load |
| CSCuo72631 | 3 | ucmap | PCD does not clear the task >status when retrying a failed task |
| CSCuo58251 | 2 | uds | UDS returning IP Address to Jabber, Cert validation browser pop-ups |
| CSCuo78788 | 2 | voice-sipstack | CUCM: crash while handling malformed SIP message |

# Open Caveats for IM and Presence Service, Release 10.5(1)

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

| Identifier | Severity | Component | Headline |
|---|---|---|---|
| CSCui28980 | 3 | ccm-serviceability | Service Restart status is abnormal |
| CSCuo46302 | 3 | config-agent | Config Agent is unable to access remote database due to duplicate values |
| CSCuo34292 | 3 | contacts | Federated contacts do not appear in roster until Cisco Jabber is restarted |
| CSCuo20224 | 3 | ctigw | Lync/MOC RCC client phone status not updated on device/line failure |
| CSCuo31845 | 3 | database | Services unable to register with dbmon causing missed change notes |
| CSCuo60051 | 3 | database | Composed presence incorrect for a user after 10.5.1.10000-6 upgrade |
| CSCui58261 | 3 | database | Upgrade from Release 8.6(3) fails if special characters are in custom status message |
| CSCuo56545 | 3 | database-imdb | Config agent core on startup |
| CSCuo68665 | 3 | epe | Composed presence offline stanza should contain a PIDF |
| CSCul87398 | 3 | epe | Licensing users for IM and Presence capabilities can cause IDS CPU to spike to 90% |
| CSCum02939 | 3 | epe | Cisco Unified Communications Manager device remains stuck in DND despite clearing DND from Jabber |
| CSCuo04714 | 3 | epe | High Availability: IMDB replication overwriting user presence after split brain recovery |
| CSCuo48936 | 3 | esp | PWS unable to send Event Notification if Endpoint registered with FQDN |
| CSCuo65402 | 3 | gui | IM and Presence Cluster Overview report missing from the System Reports page |
| CSCuo65388 | 3 | gui | IM and Presence Database Replication Debug report does not work |
| CSCuo59923 | 3 | gui | Intercluster peer presence/email domains can be inadvertently removed |
| CSCul55699 | 3 | gui-admin | Cisco Unified Presence: Rework Exception Handling to Clarify GUI Notifications Post-Upgrade |

| Identifier | Severity | Component | Headline |
|---|---|---|---|
| CSCuo17197 | 3 | gui-admin | IM and Presence menu shows CCMCIP is only for legacy (non-Jabber) which is incorrect |
| CSCuo56484 | 3 | intercluster | Intercluster service jvm crashes on server reboot |
| CSCuo35984 | 3 | intercluster | ICSA unordered processing of cupowncertificates can cause cert thrashing |
| CSCul25056 | 3 | selinux | Refresh Upgrade hangs during database install from IM and Presence Release 10.0 from pre-10.0. |
| CSCun57681 | 3 | sync-agent | Cisco Unified Communications Manager not included in processnode after upgrade from Release 9.1 to 10.0(1) |
| CSCuo37125 | 3 | vos | 'show perf list classes' error during stat of classes in CUPS |
| CSCuo56564 | 3 | vos | DRS Restore status shows failed due to a DB restore failure condition |
| CSCun59316 | 3 | xcp-router | 70% reduction in login throughput if IC peer can not be contacted |
| CSCuo65513 | 3 | xcp-router | Presence and IM broken between publisher and subscriber after upgrade |
| CSCuo04591 | 3 | xcp-router | MDNS recovery after network down taking too long |
| CSCuo45617 | 3 | xcp-s2s | Cisco XMPP Federation Connection Manager crashes |