Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 11.5(1)SU4

First Published: 2017-12-04

Last Modified: 2019-08-27

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

CONTENTS

CHAPTER 1

About this Release 1

Revision History 1

Introduction 2

Supported Versions 2

Documentation for this Release 3

CLI Commands 3

Cisco Prime License Manager 3

Encryption License Requirement for Mixed-Mode 4

Caveats 5

CHAPTER 2

Upgrades 7

Upgrade Procedures 7

Supported Upgrade and Migration Paths 7

Deployments on Cisco Media Convergence Servers Hardware 7

Deployments on Virtual Machines 8

Upgrade Path Restrictions for Release 11.5(x) 10

COP Files Required for Upgrades to Release 11.5 10

Requirements and Limitations 12

Upgrade Requirements with Standalone Prime License Manager 12

Cisco Jabber During Upgrade 12

Deprecated Phone Models 12

OS Admin Account Required for CLI-Initiated IM and Presence Upgrades 13

Rolling Back to Previous Versions 13

Upgrading with FIPS Mode Enabled 14

Upgrades with Mixed Mode Enabled Require an Encryption License 14

Database Migration Required for Upgrades with Microsoft SQL Server 15

Upgrades from 11.5(1)SU2 with Push Notifications Enabled 17

CHAPTER 3 New and Changed Features 19

AES 80-Bit Authentication Support 19

Centralized Deployment for IM and Presence 19

Cisco JTAPI Support for RHEL 7 22

Deprecated Encryption Ciphers 22

CHAPTER 4 Important Notes 25

Features and Services 25

Media Sense does not record the Consult Call with Selective Recording 25

OVA Requirements and User Capacities 25

SDL Listening Port Update Requires CTIManager Restart on all Nodes 26

Interoperability 26

AXL Requests to Unified CM Nodes 26

Cisco Unified Attendant Console Support 26

IM and Presence Service Interoperability with Expressway-C 26

Tomcat Certificate Regeneration with SAML SSO Deployment 26

IM and Presence Service 27

Intercluster Peering Not Supported with Cisco Unified Presence 8.6 27

Reset High Availability Following IM and Presence Service Node Outage 27

IM and Presence Server Pings to Jabber Are Not Configurable 27

Persistent Chat Character Limit with Microsoft SQL Server 27

Rebooting IM and Presence Subscriber Nodes 27

Miscellaneous 28

Bandwidth Allocations for 88xx SIP Phones 28

Dialed Number Analyzer does not Support Single Sign-On 28

Route Filter and Associated Route Patterns 28

CHAPTER 5 Documentation Update for Defects 29

Command Line Interface Reference Guide 29

utils dbreplication clusterreset 29

Security Guide 29

Certificates 29

System Error Messages 30

Missing Device Type ENUM Values 30

Missing Reason Codes for LastOutOfServiceInformation Alarms 30

Online Help for Cisco Unified Communications Manager 33

DHCP Subnet Setup Tips 33

Insufficient Information About Opus Codec 33

Incorrect Time Period Example 33

Insufficient Information About Time Schedule 34

Insufficient Information on LDAP User Authentication 35

Remote Destination Configuration Page In the OLH Needs To Be Updated 36

SIP Profile Field Descriptions Are Missing 36

SIP Profile Settings 36

CHAPTER 6 Configure Centralized Deployment 57

Centralized Deployment Overview 57

Centralized Cluster Deployment Architecture 59

Centralized Cluster Use Case 60

Centralized Deployment Prerequisites 61

Centralized Deployment Configuration Task Flow 62

Enable IM and Presence via Feature Group Template 64

Complete LDAP Sync on IM and Presence Central Cluster 64

Enable Users for IM and Presence via Bulk Admin 65

Add Remote Telephony Clusters 66

Configure an IM and Presence UC Service 67

Create Service Profile for IM and Presence 68

Disable Presence Users in Telephony Cluster 68

Configure OAuth Refresh Logins 69

Configure an ILS Network 70

Configure Cluster IDs for ILS 71

Enable ILS on Telephony Clusters 71

Verify ILS Network is Running 72

MRA Configuration 73

Centralized Deployment Field Descriptions 74

Centralized Deployment Interactions and Restrictions 74

CHAPTER 7 **Migrate Users to Centralized Deployment** 77

Centralized Deployment User Migration Overview 77

Prerequisite Tasks for Central Cluster Migration 77

Migration to Central Cluster Task Flow 78

Export Contact Lists from Migrating Cluster 80

Disable High Availability in Migrating Cluster 81

Configure UC Service for IM and Presence 82

Create Service Profile for IM and Presence 82

Disable Presence Users in Telephony Cluster 83

Enable OAuth Authentication for Central Cluster 84

Disable High Availability in Central Cluster 84

Delete Peer Relationship for Central and Migrating Clusters 85

Stop the Cisco Intercluster Sync Agent 85

Enable IM and Presence via Feature Group Template 86

Complete LDAP Sync on Central Cluster 86

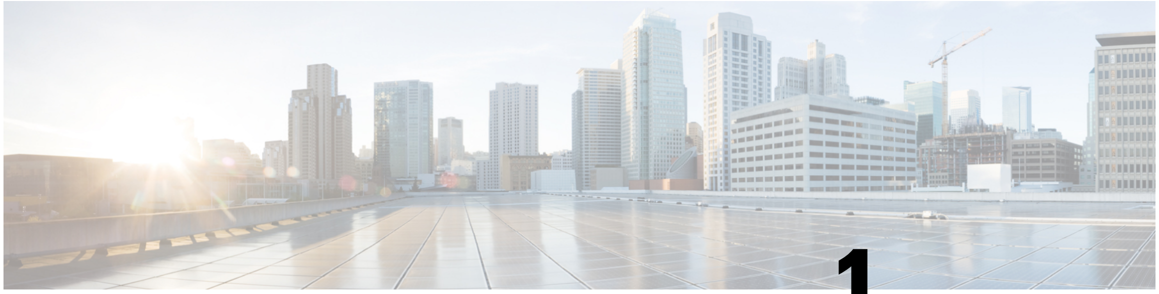
Enable Users for IM and Presence via Bulk Admin 87

Import Contact Lists into Central Cluster 88

Start Cisco Intercluster Sync Agent 89

Enable High Availability in Central Cluster 89

Delete Remaining Peers for Migrating Cluster 90



CHAPTER 1

About this Release

- Revision History, on page 1
- Introduction, on page 2
- Supported Versions, on page 2
- Documentation for this Release, on page 3
- CLI Commands, on page 3
- Cisco Prime License Manager, on page 3
- Encryption License Requirement for Mixed-Mode, on page 4
- Caveats, on page 5

Revision History

Date	Revision
June 07, 2019	Added link to Caveats in the Readme file.
February 15, 2018	Initial publish
March 26, 2018	Removed HTTPS Proxy feature while support is being testing and verified. Feature will be reinserted after testing is completed and support is verified.
March 28, 2018	Updated the Prerequisites for the IM and Presence Centralized Deployment feature.
April 09, 2018	Added Important Notes section and Documentation Updates section. Added SIP Profile Settings topic around online help.
April 08, 2019	Added migration chapter for Centralized Deployment. Also updated OVA requirements for IM+P.
May 28, 2019	Updated Centralized Deployment migration requirements.

Introduction

These release describe new features, restrictions, and caveats for Cisco Unified Communications Manager (Unified Communications Manager) and Cisco Unified Communications Manager IM & Presence Service (IM and Presence Service). The 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. It helps employees connect with colleagues more efficiently and determine the most effective way to engage in collaborative communication.

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

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.

Supported Versions

The following versions are supported for this release:

- Cisco Unified Communications Manager 11.5.1.14900-11
- IM and Presence Service 11.5.1.14900-32

Version Mismatches

This release offers two main deployment options for this release of Cisco Unified Communications Manager and the IM and Presence Service:

- Standard Deployments—Both Cisco Unified Communications Manager and the IM and Presence Service must be running the above 11.5(1)SU4 version for your deployment to be supported. A version mismatch is not supported.
- Centralized Deployments of IM and Presence Service—If you have the Centralized Deployment option configured on the IM and Presence Service, then within the IM and Presence central cluster, both the Cisco Unified Communications Manager instance and the IM and Presence Service must be running a 11.5(1)SU4 version. However, the telephony cluster that the central cluster connects to does not have to be running a 11.5(1)SU4 version.

Documentation for this Release

Aside from these Release Notes, the following documents were updated specifically for Release 11.5(1)SU4 of Cisco Unified Communications Manager and the IM and Presence Service:

Documents	Description
ReadMe Files for 11.5(1)SU4: • ReadMe for Cisco Unified Communications Manager Release 11.5(1)SU4 • ReadMe for Cisco Unified IM and Presence, Release 11.5(1)SU4	Refer to the Readme for information on installing and deploying the release, as well as bug fixes and updates that are includes in your release
Deploying Push Notifications for Cisco Jabber on iPhone and iPad with Cisco Unified Communications Manager 11.5(1)SU4	This solution document is updated for 11.5(1)SU4. The document describes the Push Notifications solution for Cisco Jabber on iPhone and iPad. As of this release, this solution now supports push notifications for voice and video calls as well as IM and Presence.

Existing 11.5(x) Documentation

Existing documents for Release 11.5(x) can be used for 11.5(1)SU4. Refer to the *Documentation Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5(1)* at the below URL for a full listing of the documentation that is available. Where an 11.5(1)SU version exists where the SU is equivalent to, or lower than, SU4, you should use that document version. Otherwise, you can use the 11.5(1) version.

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/docguide/11_5_1/cucm_b_documentation-guide-cucm-imp-1151.html

CLI Commands

For a complete list of CLI commands that are available with this release, refer to the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions, Release 11.5(1)SU3* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Cisco Prime License Manager

Cisco Unified Communications Manager Release 11.5(1)SU3, SU4, SU5, and SU6 are compatible with Cisco Prime License Manager Release 11.5(1)SU2 or higher. If you are deploying a standalone Cisco Prime License Manager, make sure that your Prime License Manager version is a minimum release of 11.5(1)SU2. Otherwise, Cisco Unified Communications Manager cannot synchronize its license usage with the standalone Prime License Manager.

If you are upgrading to one of these Cisco Unified Communications Manager releases and you are running a standalone version of Prime License Manager, upgrade your Prime License Manager instance to 11.5(1)SU2 or higher before you upgrade Cisco Unified Communications Manager.

Note With co-resident Prime License Manager deployments, Cisco Unified Communications Manager and Cisco Prime License Manager are compatible automatically.

Encryption License Requirement for Mixed-Mode

This release of Cisco Unified Communications Manager introduces support for encryption licenses. If you want to enable mixed-mode in Cisco Unified Communications Manager, you must have an encryption license installed in Cisco Prime License Manager and applied against Cisco Unified Communications Manager.

Fresh Installations

Upon installing your cluster, you will be unable to move the cluster into mixed-mode unless you have an encryption license applied against Cisco Unified Communications Manager, and a sync has been completed. If you do not have an encryption license, and you attempt to move the cluster into mixed-mode, an empty CTL file will be generated and the cluster will remain in non-secure mode.

Upgrades

If you upgrade from an earlier release with mixed-mode enabled, but you do not have an encryption license installed, a warning message on the encryption license requirement displays on the user interface immediately followng the upgrade. You will also receive the **CiscoSystemEncryptionNotAllowed** alert. Your system will continue to operate in mixed-mode, but you will be unable to update the CTL file and will continue to receive this alert until you either install an encryption license or move the cluster security setting back to non-secure mode. Cisco recommends that you install the encryption license at the earliest to ensure that you can continue to run mixed mode without any disruption.

If you were not running mixed-mode prior to the upgrade, you will be unable to move the cluster into mixed-mode unless you have an encryption license applied against Cisco Unified Communications Manager, and a sync has been completed.

User Interface Updates

In the Cisco Unified CM Administration interface's **License Usage Report** window, a new field has been added to the **Cisco Prime License Manager** section:

- **Encryption License installed**—This field contains a **True** or **False** value that indicates whether an encryption license is installed.

Ordering and Installing License Files

The following table describes how to update your system with an encryption license.

Table 1: Updating your System with an Encryption License

Step	Task	Description
Step 1	Obtain an ENC PAK license file.	Use the CUCM-PLM-ENC-K9= part number to order encryption licenses via the Product Upgrade Tool at https://tools.cisco.com/gct/Upgrade/jsp/index.jsp. For further information on ordering licenses, refer to the *Cisco Unified Communications Solutions Ordering Guide* for your release at http://www.cisco.com/c/en/us/partners/tools/collaboration-ordering-guides.html. **Note** If you are using multiple instances of Cisco Prime License Manager in your deployment, you must order a separate encryption license for each Prime License Manager instance.
Step 2	Install the encryption license file in Cisco Prime License Manager.	Follow the "Upgrade Existing Licenses" procedure in the *Cisco Prime License Manager User Guide, Release 11.5(1)SU2* at http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-license-manager/products-user-guide-list.html.
Step 3	Synchronize licenses.	In Cisco Prime License Manager, select the **Product Instances** tab and click **Synchronize licenses**. For additional detail, see the *Cisco Prime License Manager User Guide, Release 11.5(1)SU2*.

Caveats

For a list of open and resolved caveats for this release, refer to the following files:

- Readme File for Cisco Unified Communications Manager, Release 11.5(1)SU4
- Readme File for Cisco Unified CM IM and Presence Service, Release 11.5(1)SU4

CHAPTER 2

Upgrades

- Upgrade Procedures, on page 7
- Supported Upgrade and Migration Paths, on page 7
- Requirements and Limitations, on page 12

Upgrade Procedures

For detailed procedures on how to upgrade your system, refer to the *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5(1)* at the following URL:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/upgrade/11_5_1/cucm_b_upgrade-guide-cucm-115.html

Supported Upgrade and Migration Paths

Use the following tables to determine whether you can upgrade or migrate from your currently installed version, and which of the supported upgrade methods are available to you:

- Direct upgrades using either the Cisco Unified CM OS Admin interface or the Cisco Prime Collaboration Deployment (PCD) Upgrade task
- Migrations using the PCD Migration task

If an upgrade or migration from your current release is not supported, see the instructions in the "Upgrading from Legacy Releases" chapter of the *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service*.

Deployments on Cisco Media Convergence Servers Hardware

You cannot install or run Cisco Unified Communications Manager and the IM and Presence Service directly on server hardware; you must run these applications on virtual machines. The tables below list the supported migration paths for deployments that are currently running on Cisco 7800 Series Media Convergence Server (MCS 7800) hardware. All of the supported migration paths listed below are physical-to-virtual (P2V) migrations.

Note The tables below list the upgrade paths supported for MCS 7800 Series servers, with the following exceptions:

- MCS 7816-C1 for Business Edition 3000 (BE3000)
- MCS 7828 for Business Edition 5000 (BE5000)

PCD migrations are not supported for BE3000 and BE5000 deployments. We recommend a fresh installation for upgrades from these products.

Table 2: Unified Communications Manager Releases Installed on MCS 7800 Series Hardware

From	To	Supported Method
6.1(5)	11.5(x)	PCD Migration
7.1(3) and 7.1(5)	11.5(x)	PCD Migration
8.x	11.5(x)	PCD Migration
9.x	11.5(x)	PCD Migration

Table 3: Cisco Unified Presence and IM and Presence Releases Installed on MCS 7800 Series Hardware

From	To	Supported Method
CUP 8.5(4)	11.5(x)	PCD Migration
CUP 8.6(3), 8.6(4), and 8.6(5)	11.5(x)	PCD Migration
IM and Presence 9.x	11.5(x)	PCD Migration

Deployments on Virtual Machines

The tables below list the supported upgrade and migration paths for Cisco Unified Communications Manager and IM and Presence Service deployments that are currently running on virtual machines. All of the supported upgrade and migration paths listed below are virtual-to-virtual (V2V). Service Updates (SU) within each path are supported, unless otherwise indicated.

Table 4: Unified Communications Manager Releases Installed on Virtual Machines

From	To	Supported Method
8.6(x)	11.5(x)	Cisco Unified OS Admin (Direct Refresh) PCD Migration PCD Upgrade (Direct Refresh)
9.0(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Refresh)

From	To	Supported Method
9.1(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Refresh) Cisco Unified OS Admin (Direct Refresh)
10.0(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Standard)
10.5(x) **Note** Exceptions exist for some 10.5(2) SU releases; see Upgrade Path Restrictions for Release 11.5(x), on page 10 for more information.	11.5(x)	PCD Migration PCD Upgrade (Direct Standard) Cisco Unified OS Admin (Direct Standard)
11.0(1)	11.5(x)	Cisco Unified OS Admin (Direct Standard) PCD Migration PCD Upgrade (Direct Standard)
11.5(x)	11.5(y)	Cisco Unified OS Admin (Direct Standard) PCD Migration PCD Upgrade (Direct Standard)

Table 5: Cisco Unified Presence and IM and Presence Releases Installed on Virtual Machines

From	To	Supported Method
CUP 8.5(4)	11.5(x)	PCD Migration
CUP 8.6(3), 8.6(4), and 8.6(5)	11.5(x)	PCD Migration PCD Upgrade (Direct Refresh)
CUP 8.6(x)	11.5(x)	Cisco Unified OS Admin (Direct Refresh)
IM and Presence 9.0(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Refresh)
IM and Presence 9.1(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Refresh) Cisco Unified OS Admin (Direct Refresh)

From	To	Supported Method
IM and Presence 10.0(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Standard) PCD Upgrade (Direct Standard)
IM and Presence 10.5(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Standard) Cisco Unified OS Admin (Direct Standard)
IM and Presence 11.0(1)	11.5(x)	Cisco Unified OS Admin (Direct Standard) PCD Migration PCD Upgrade (Direct Standard)
IM and Presence 11.5(x)	11.5(y)	Cisco Unified OS Admin (Direct Standard) PCD Migration PCD Upgrade (Direct Standard)

Upgrade Path Restrictions for Release 11.5(x)

Upgrade and migration paths generally support the Service Updates (SU) within each path; however, there are some exceptions for specific SU releases. The table below lists the exceptions for upgrades and migrations to Cisco Unified Communications Manager Release 11.5(x).

Table 6: Restrictions to Supported Upgrade and Migration Paths, Cisco Unified Communications Manager Release 11.5(x)

From	To	Description
10.5(2)SU5	11.5(1.10000-6) through 11.5(1.120xx)	Path is unsupported. For these releases, upgrade to 11.5(1)SU2 instead.

COP Files Required for Upgrades to Release 11.5

The tables below lists the upgrade paths that require COP files. You must install COP files on each node before you begin an upgrade using the Cisco Unified OS Admin interface, or before you begin an upgrade or migration using the Prime Collaboration Deployment (PCD) tool. If you are using PCD, you can perform a bulk installation of the COP files before you begin the upgrade.

Table 7: Required COP Files for Upgrades and Migrations to Cisco Unified Communications Manager Release 11.5(x)

From	To	Upgrade Type
8.6(x)	11.5(x)	Refresh upgrade. Required COP files: • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
9.1(x)	11.5(x)	Refresh upgrade. Required COP files: • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
10.5(x)	11.5(x)	Standard upgrade; no COP file required.
11.0(x)	11.5(x)	Standard upgrade; no COP file required.
11.5(x)	11.5((y)	Standard upgrade; no COP file required.

Table 8: Required COP Files for Refresh Upgrades from Cisco Unified Presence Releases

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
8.5(4) through 8.6(1)	11.5(x)	Refresh upgrade. Requires the following COP files: • cisco.com.cup.refresh_upgrade_v<latest_version>.cop • ciscocm.version3-keys.cop.sgn

Table 9: Required COP Files for Refresh Upgrades from IM and Presence Service Releases

From IM and Presence Release	To IM and Presence Release	Upgrade Type
9.1(x)	11.5(x)	Refresh upgrade. Requires the following COP file: • ciscocm.version3-keys.cop.sgn
10.5(x)	11.5(x)	Standard upgrade; no COP file required.
11.0(x)	11.5(x)	Standard upgrade; no COP file required.
11.5(x)	11.5(y)	Standard upgrade; no COP file required.

Requirements and Limitations

This section contains requirements and limitations to consider when upgrading your system.

Upgrade Requirements with Standalone Prime License Manager

Cisco Unified Communications Manager Release 11.5(1)SU3, SU4, SU5, and SU6 are compatible with Cisco Prime License Manager Release 11.5(1)SU2 or higher. If you are deploying a standalone Cisco Prime License Manager, make sure that your Prime License Manager version is a minimum release of 11.5(1)SU2. Otherwise, Cisco Unified Communications Manager cannot synchronize its license usage with the standalone Prime License Manager.

If you are upgrading to one of these Cisco Unified Communications Manager releases and you are running a standalone version of Prime License Manager, upgrade your Prime License Manager instance to 11.5(1)SU2 or higher before you upgrade Cisco Unified Communications Manager.

Note With co-resident Prime License Manager deployments, Cisco Unified Communications Manager and Cisco Prime License Manager are compatible automatically.

Cisco Jabber During Upgrade

It is not essential requirement that all users must log out from Cisco Jabber, when upgrading the IM and Presence Service. However, it is always a best practice that users are log out from Cisco Jabber during the upgrade.

Deprecated Phone Models

Upgrades that Involve Deprecated Phones

If you are using any of these phones on an earlier release and you want to upgrade to this release, do the following:

1. Confirm whether the phones in your network will be supported in Release 11.5.

2. Identify any non-supported phones.

3. For any non-supported phones, power down the phone and disconnect the phone from the network.

4. Provision a supported phone for the phone user. You can use the Migration FX tool to migrate from older model to newer model phones. For details, go to: http://refreshcollab.cisco.com/webportal/46/CUCM%20Readiness%20Assessment#endpoint_refresh_tool.

5. Once all the phones in your network are supported by Release 11.5, upgrade your system.

Note Deprecated phones can also be removed after the upgrade. When the administrator logs in to Cisco Unified Communications Manager after completing the upgrade, the system displays a warning message notifying the administrator of the deprecated phones.

Licensing

You do not need to purchase a new device license to replace a deprecated phone with a supported phone. The device license becomes available for a new phone when you either remove the deprecated phone from the system, or when you switch to the new Cisco Unified Communications Manager version, and the deprecated phone fails to register.

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

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

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

Rolling Back to Previous Versions

Standard Deployments of IM and Presence

With Standard Deployments of the IM and Presence Service, if you run into any upgrade issues and you need to roll back to a previous version, you must roll back both the Cisco Unified Communications Manager and the IM and Presence Service installations to the previous version or you will have a non-supported version mismatch.

It's not supported with Standard Deployments to roll back the Cisco Unified Communications Manager version and leave the IM and Presence Service version at 11.5(1)SU4. Similarly, it's not supported to roll back the IM and Presence Service version and leave the Cisco Unified Communications Manager version at 11.5(1)SU4.

Centralized Deployment Exception

The exception to this rule is with the IM and Presence Centralized Deployment because IM and Presence and telephony are hanlded by different clusters. Within the IM and Presence central cluster, the Cisco Unified Communications Manager database instance must be running the same version as the IM and Presence Service. However, the separate telephony cluster to which the IM and Presence Service connects can be running a different version.

Upgrading with FIPS Mode Enabled

For Release 11.5(x), Cisco Unified Communications Manager and IM and Presence Service do not support RSA certificates with key-sizes that are less than 2048 bits when FIPS mode is enabled. This affects server certificates and LSCs.

If you are upgrading to Release 11.5(x) with FIPS mode enabled and you are using RSA key-sizes that are less than 2048 bits on your current version, then you can carry out one of the following items to resolve the problem.

You can either:

- Regenerate the effected certificates before you upgrade if your current version supports key-sizes of 2048 bits, or
- Regenerate the effected certificates after you upgrade to Release 11.5(x).

Note If you choose this option, then secure connections are not allowed to use the effected certificates until they have an RSA key-size of 2048 bits or greater.

Upgrades with Mixed Mode Enabled Require an Encryption License

This release requires that you have an encryption license installed in order to run Cisco Unified Communications Manager in mixed mode. If you are upgrading from an earlier release of Cisco Unified Communications Manager, and cluster security is set to mixed-mode, you must obtain an encryption license and install it in Cisco Prime License Manager.

If you upgrade from an earlier release with mixed-mode enabled, but you do not have an encryption license installed, a warning message on the encryption license requirement displays on the user interface immediately followng the upgrade. You will also receive the **CiscoSystemEncryptionNotAllowed** alert. Your system will continue to operate in mixed-mode, but you will be unable to update the CTL file and will continue to receive this alert until you either install an encryption license or move the cluster security setting back to non-secure mode. Cisco recommends that you install the encryption license at the earliest to ensure that you can continue to run mixed mode without any disruption.

If you were not running mixed-mode prior to the upgrade, you will be unable to move the cluster into mixed-mode unless you have an encryption license applied against Cisco Unified Communications Manager, and a sync has been completed.

Ordering and Installing License Files

The following table describes how to update your system with an encryption license.

Table 10: Updating your System with an Encryption License

Step	Task	Description
Step 1	Obtain an ENC PAK license file.	Use the CUCM-PLM-ENC-K9= part number to order encryption licenses via the Product Upgrade Tool at https://tools.cisco.com/gct/Upgrade/jsp/index.jsp. For further information on ordering licenses, refer to the *Cisco Unified Communications Solutions Ordering Guide* for your release at http://www.cisco.com/c/en/us/partners/tools/collaboration-ordering-guides.html. **Note** If you are using multiple instances of Cisco Prime License Manager in your deployment, you must order a separate encryption license for each Prime License Manager instance.
Step 2	Install the encryption license file in Cisco Prime License Manager.	Follow the "Upgrade Existing Licenses" procedure in the *Cisco Prime License Manager User Guide, Release 11.5(1)SU2* at http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-license-manager/products-user-guide-list.html.
Step 3	Synchronize licenses.	In Cisco Prime License Manager, select the **Product Instances** tab and click **Synchronize licenses**. For additional detail, see the *Cisco Prime License Manager User Guide, Release 11.5(1)SU2*.

Database Migration Required for Upgrades with Microsoft SQL Server

If you have Microsoft SQL Server deployed as an external database with the IM and Presence Service and you are upgrading from 11.5(1), 11.5(1)SU1, or 11.5(1)SU2, you must create a new SQL Server database and migrate to the new database. This is required due to enhanced data type support in this release. If you don't migrate your database, schema verification failure will occur on the existing SQL Server database and services that rely on the external database, such as persistent chat, will not start.

After you upgrade your IM and Presence Service, use this procedure to create a new SQL Server database and migrate data to the new database.

Note This migration is not required for Oracle or PostgreSQL external databases.

Before You Begin

The database migration is dependent on the `MSSQL_migrate_script.sql` script. Contact Cisco TAC to obtain a copy.

Table 11:

Step	Task
Step 1	Create a snapshot of your external Microsoft SQL Server database.
Step 2	Create a new (empty) SQL Server database. For details, see the following chapters in the *Database Setup Guide for the IM and Presence Service*: **1.** "Microsoft SQL Installation and Setup"—Refer to this chapter for details on how to create your new SQL server database on your upgraded IM and Presence Service. **2.** "IM and Presence Service External Database Setup"—After your new database is created, refer to this chapter to add the database as an external database in the IM and Presence Service.
Step 3	Run the System Troubleshooter to confirm that there are no errors with the new database. **1.** From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**. **2.** Verify that no errors appear in the **External Database Troubleshooter** section.
Step 4	Restart the Cisco XCP Router on all IM and Presence Service cluster nodes: **1.** From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**. **2.** From the **Server** menu, select an IM and Presence Service node and click **Go**. **3.** Under **IM and Presence Services**, select **Cisco XCP Router** and click **Restart**.
Step 5	Turn off services that depend on the external database: **1.** From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Feature Services**. **2.** From the **Server** menu, select an IM and Presence node and click **Go**. **3.** Under **IM and Presence Services**, select the following services:. Cisco XCP Text Conference Manager Cisco XCP File Transfer Manager Cisco XCP Message Archiver **4.** Click **Stop**.
Step 6	Run the following script to migrate data from the old database to the new database `MSSQL_migrate_script.sql`. **Note** Contact Cisco TAC to obtain a copy of this script

Step	Task
Step 7	Run the System Troubleshooter to confirm that there are no errors with the new database. 1. From Cisco Unified CM IM and Presence Administration, choose **Diagnostics** > **System Troubleshooter**. 2. Verify that no errors appear in the **External Database Troubleshooter** section.
Step 8	Start the services that you stopped previously. 1. From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Feature Services**. 2. From the **Server** menu, select an IM and Presence node and click **Go**. 3. Under **IM and Presence Services**, select the following services: Cisco XCP Text Conference Manager Cisco XCP File Transfer Manager Cisco XCP Message Archiver 4. Click **Start**.
Step 9	Confirm that the external database is running and that all chat rooms are visible from a Cisco Jabber client. Delete the old database only after you're confident that the new database is working.

Upgrades from 11.5(1)SU2 with Push Notifications Enabled

If you are upgrading from the 11.5(1)SU2 release and you had Push Notifications enabled in the old release, you must disable Push Notifications in the current release and then follow the onboarding process to enable Push Notifications once again. This is required due to API changes in this release that were not a part of the 11.5(1)SU2 release. Your upgraded system will not be able to send troubleshooting logs to the Cisco Cloud unless you disable Push Notifications and then follow the onboarding process for this release.

After you upgrade your system, do the following:

Procedure

Step 1 Disable Push Notifications

Follow these steps:

1. From Cisco Unified CM Administration, choose **Advanced Features** > **Cisco Cloud Onboarding**
2. Uncheck the following check boxes:
   - **Enable Push Notifications**
   - **Send Troubleshooting information to the Cisco Cloud**
   - **Send encrypted PII to the Cisco Cloud for troubleshooting**

3. Click **Save**.

Step 2 Enable Push Notifications for this release.

For the full onboarding process, see the "Push Notifications Configuration Task Flow" in the *Deploying Push Notifications for Cisco Jabber on iPhone and iPad* document at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/pushNotifications/11_5_1_su2/cucm_b_push-notification-deployment-iPhone-iPad.html.

CHAPTER 3

New and Changed Features

- AES 80-Bit Authentication Support, on page 19
- Centralized Deployment for IM and Presence, on page 19
- Cisco JTAPI Support for RHEL 7, on page 22
- Deprecated Encryption Ciphers, on page 22

AES 80-Bit Authentication Support

Cisco Unified Communications Manager supports Advanced Encryption Standard (AES) with a 128-bit encryption key and a 32-bit authentication tag used as the encryption cipher. With this release, the AES 32-bit authentication tag is enhanced to an 80-bit authentication tag used as the encryption cipher on Music On Hold (MOH), Interactive Voice Response (IVR), and Annunciator. This enhancement helps customers using 80-bit authentication tag to make the Secure Real-Time Transport Protocol (SRTP) calls over a SIP line and SIP trunk.

For more information, see the Encrypted Phone Configuration File Setup chapter in the *Security Guide for Cisco Unified Communications Manager*.

Centralized Deployment for IM and Presence

The IM and Presence centralized deployment allows you to deploy your IM and Presence deployment and your telephony deployment in separate clusters. The central IM and Presence cluster handles IM and Presence for the enterprise, while the remote Cisco Unified Communications Manager telephony cluster handles voice and video calls for the enterprise.

The Centralized Deployment option provides the following benefits when compared to standard deployments:

- The Centralized Deployment option does not require a 1x1 ratio of telephony clusters to IM and Presence Service clusters–you can scale your IM and Presence deployment and your telephony deployment separately, to the unique needs of each.
- Full mesh topology is not required for the IM and Presence Service
- Version independent from telephony–your IM and Presence central cluster can be running a different version than your Cisco Unified Communications Manager telephony clusters.
- Can manage IM and Presence upgrades and settings from the central cluster.

- Lower cost option, particularly for large deployments with many Cisco Unified Communications Manager clusters
- Easy XMPP Federation with third parties.
- Supports calendar integration with Microsoft Outlook. For configuration details, refer to the document *Microsoft Outlook Calendar Integration for the IM and Presence Service*.

Centralized Deployment Setup vs Standard (Decentralized) Deployments

The following table discusses some of the differences in setting up an IM and Presence Centralized Cluster Deployment as opposed to standard deployments of the IM and Presence Service.

Setup Phase	Differences with Standard Deployments
Installation Phase	The installation process for an IM and Presence central deployment is the same as for the standard deployment. However, with central deployments, the IM and Presence central cluster is installed separatelyfrom your telephony cluster, and may be located on separate hardware servers. Depending on how you plan your topology, the IM and Presence central cluster may be installed on separate physical hardware from your telephony cluster. For the IM and Presence central cluster, you must still install Cisco Unified Communications Manager and then install the IM and Presence Service on the same servers. However, the Cisco Unified Communications Manager instance of the IM and Presence central cluster is for database and user provisioning primarily, and does not handle voice or video calls.

Setup Phase	Differences with Standard Deployments
Configuration Phase	Compared to standard (decentralized) deployments, the following extra configurations are required to set up the IM and Presence Service Central Deployment: • Users must be synced into both the telephony cluster and the IM and Presence Service central cluster so that they exist in both databases. • In your telephony clusters, end users should not be enabled for IM and Presence. • In your telephony clusters, the Service Profile must include the IM and Presence Service and must point to the IM and Presence central cluster. • In the IM and Presence central cluster, users must be enabled for the IM and Presence Service. • In the IM and Presence central cluster's database publisher node, add your remote Cisco Unified Communications Manager telephony cluster peers. The following configurations, which are used with Standard Deployments of the IM and Presence Service, but are not required with Central Deployments: • A Presence Gateway is not required. • A SIP Publish trunk is not required. • A Service Profile is not required on the IM and Presence central cluster—the Service Profile is configured on the telephony cluster to which the central cluster connects

The IM and Presence centralized deployment allows you to deploy your IM and Presence deployment and your telephony deployment in separate clusters. The central IM and Presence cluster handles IM and Presence for the enterprise, while the remote Cisco Unified Communications Manager telephony cluster handles voice and video calls for the enterprise.

The Centralized Deployment option provides the following benefits when compared to standard deployments:

- The Centralized Deployment option does not require a 1x1 ratio of telephony clusters to IM and Presence Service clusters–you can scale your IM and Presence deployment and your telephony deployment separately, to the unique needs of each.
- Full mesh topology is not required for the IM and Presence Service
- Version independent from telephony–your IM and Presence central cluster can be running a different version than your Cisco Unified Communications Manager telephony clusters.
- Can manage IM and Presence upgrades and settings from the central cluster.
- Lower cost option, particularly for large deployments with many Cisco Unified Communications Manager clusters
- Easy XMPP Federation with third parties.
- Supports calendar integration with Microsoft Outlook. For configuration details, refer to the document *Microsoft Outlook Calendar Integration for the IM and Presence Service*.

Interclustering for Centralized Deployment

Interclustering is supported between two centralized clusters. Intercluster peering is tested with one cluster with 25K (with 25K OVA) and another with 15K (with 15K OVA) devices and no performance issues were observed.

User Interface Updates

To manage this feature, the **Centralized Deployment** window has been added to the **System** menu of the Cisco Unified CM IM and Presence Administration interface. Administrators can add their remote Cisco Unified Communications Manager clusters to the IM and Presence central cluster in this window.

Configuration

For information on configuring a newly installed system for the Centralized Deployment, see the supplementary Configure Centralized Deployment, on page 57 chapter.

For information on migrating to a Centralized Deployment cluster, see the supplementary Migrate Users to Centralized Deployment , on page 77.

Cisco JTAPI Support for RHEL 7

With this release, Cisco Unified JTAPI supports Red Hat Enterprise Linux 7 for 64-bit on the Linux operating system. Previously, it supported RHEL 6.

Support for VMware

Cisco JTAPI is used on VMware ESXi version 4.0. The application uses Windows 2003 and Windows 2008 virtual machines on the VMware version to run Cisco KJTAPI

Cisco JTAPI Documentation

For more details on Cisco Unified JTAPI, see the “Features Supported by Cisco Unified JTAPI” chapter in the *Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html.

Deprecated Encryption Ciphers

To ensure that your system security keeps pace with today's standards, support for some weaker encryption ciphers has been removed. System components that use data encryption such as CAPF, SSH and TVS have been tested so that weaker ciphers can be removed from the supported list.

The following 3DES ciphers are no longer supported with your system:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

In addition, the following ciphers are still supported by default. However, if you enable TLS version 1.2, these ciphers are also not supported:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

CHAPTER 4

Important Notes

- Features and Services, on page 25
- Interoperability, on page 26
- IM and Presence Service, on page 27
- Miscellaneous, on page 28

Features and Services

Media Sense does not record the Consult Call with Selective Recording

When Selective Recording is configured, the Media Sense server does not record the consult call during a transfer. For example, if a call between an agent and a customer is being recorded, and the agent initiates a transfer to another agent, the consult call that takes place between the two agents, prior to the call being transferred, is not recorded.

To ensure that the consult call is recorded, the agent must press the ‘Record’ softkey when the consult call starts.

OVA Requirements and User Capacities

When sizing your deployment, keep these guidelines in mind around OVA requirements:

- For multi-cluster deployments, we recommend that you deploy a minimum OVA of 15,000 users
- For Persistent Chat deployments, we recommend that you deploy a minimum OVA of 15,000 users
- For Centralized deployments, we recommend a minimum OVA of 25,000 users

Note If you plan to enable Multiple Device Messaging, measure deployments by the number of clients instead of by the number of users as each user may have multiple Jabber clients. For example, if you have 25,000 users, and each user has two Jabber clients, your deployment must have the capacity of 50,000 users.

SDL Listening Port Update Requires CTIManager Restart on all Nodes

Note that if you edit the setting of the **SDL Listening Port** service parameter, you must restart the **Cisco CTIManager** service on all cluster nodes where the service is running. Currently, the help text says to restart the service, but does not specify that you must restart the service on all nodes where the service is running. You can access this service parameter from Cisco Unified CM Administration by going to **System** > **Service Parameters**, selecting **Cisco CTIManager** as the service, and clicking **Advanced** to see a complete list of CTIManager service parameters.

This update is a part of CSCvp56764.

Interoperability

AXL Requests to Unified CM Nodes

If you run Cisco TelePresence Management Suite (TMS) for scheduling, then the node that you add it to sends multiple AXL queries to fetch endpoint information. Because of the load that TMS generates, we recommend that you do not configure other applications that use AXL (such as Cisco Emergency Responder or Cisco Unified Attendant Console) to send AXL requests to these nodes.

Cisco Unified Attendant Console Support

This information applies to CSCva12833.

Cisco Unified Attendant Console Releases 11.x and earlier are not compatible with Cisco Unified Communications Manager Release 11.5(1). You must install or upgrade to Cisco Unified Attendant Console Advanced Release 11.0.1.

See here for more information.

IM and Presence Service Interoperability with Expressway-C

To interoperate Cisco Unified IM and Presence Service Release 11.5(1) and Expressway-C, you must be running a minimum version of Expressway-C X8.8. IM and Presence Service 11.5(1) does not support earlier versions of Expressway-C.

If you are upgrading from an earlier release where you are already interoperating with Expressway-C, upgrade your Expressway-C system to X8.8. After upgrading Expressway-C, you can upgrade your IM and Presence Service.

Tomcat Certificate Regeneration with SAML SSO Deployment

If you regenerate Tomcat certificates within a SAML SSO Deployment, you must also generate a new metadata file in Cisco Unified Communications Manager and upload that metadata file to the IdP.

IM and Presence Service

Intercluster Peering Not Supported with Cisco Unified Presence 8.6

Cisco Unified Presence 8.6 is not supported as an intercluster peer for Cisco Unified IM and Presence Service 11.x. For information on supported intercluster peer configurations, see the *Compatibility Matrix for Cisco Unified Communications Manager and IM and Presence Service* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/11_x/cucm_b_cucm-imp-compatibility-matrix-11x.html#CUP0_RF_I0092C6B_00.

Reset High Availability Following IM and Presence Service Node Outage

This documentation update addresses CSCuz86028.

During an IM and Presence Service node outage, caused for example by a node reboot or a node network outage. If this results in a High Availability failover, ensure that after fallback has occurred that you reset High Availability (HA).

You can do this by first disabling HA and then enabling HA on the **Presence Redundancy Groups Configuration** window on Cisco Unified Communications Manager.

IM and Presence Server Pings to Jabber Are Not Configurable

IM and Presence server updates the presence status of the user as Unavailable if it does not receive a keep-alive from the client after two 1-minute pings.

The timings for these pings are hard-coded on the server side and are not configurable.

Persistent Chat Character Limit with Microsoft SQL Server

If you have Persistent Chat configured with Microsoft SQL Server as the external database, chat messages where the total message body (HTML tags + text message) exceeds 4000 characters are rejected and are not delivered. See CSCvd89705 for additional detail. This issue exists from Release 11.5(1)SU3 onward.

Rebooting IM and Presence Subscriber Nodes

If the Cisco Unified Communications Manager and IM and Presence Service publisher nodes are both unavailable, such as may occur in a UCS server crash, do not restart any IM and Presence Service subscriber nodes as the subscriber node may not recover, and Jabber users may not be able to log in, thereby requiring a rebuild of the IM and Presence cluster.

Make sure to get the Cisco Unified Communications Manager and IM and Presence Service publisher nodes up and running before you restart any IM and Presence subscriber nodes.

Miscellaneous

Bandwidth Allocations for 88xx SIP Phones

If you are deploying 88xx phones with the SIP protocol, note that these phones will use more bandwidth than the recommended 32 kbps while registering to Cisco Unified Communications Manager. Make sure to take account for the higher bandwidth requirement over registration when you configure your QoS bandwidth allocation in the APIC-EM Controller.

Dialed Number Analyzer does not Support Single Sign-On

Dialed Number Analyzer does not support Single Sign-On

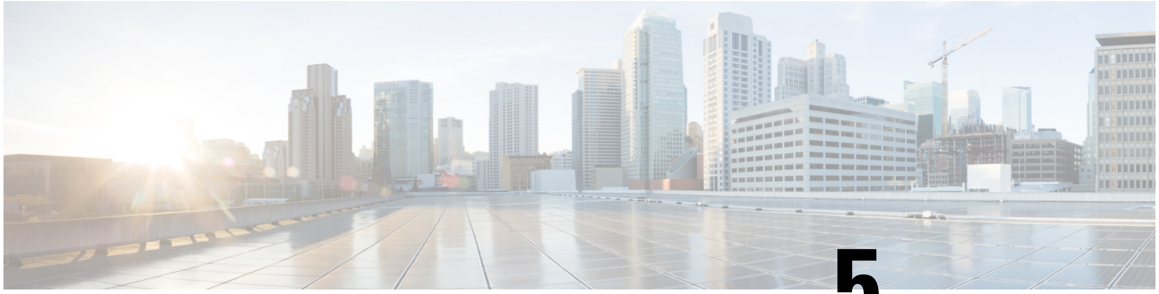
Dialed Number Analyzer (DNA), installed, as a service feature on Cisco Unified Communications Manager, does not support Single Sign-On (SSO). Use non-SSO mode to log into the application. After you log in using a non-SSO mode, you can access Cisco Unified Communications Manager Administration without an SSO login.

To access DNA, enter the following URL in your web browser:

https://<cm-machine>/dna, where <cm-machine> is the node name or IP address on which Dialed Number Analyzer is installed.

Route Filter and Associated Route Patterns

When configuring your call routing, make sure that you don't assign a single route filter to too many route patterns. A system core could result if you were to edit a route filter that has hundreds of associated route patterns, due to the extra system processing that is required to update call routing for all of the route patterns that use the route filter. Create duplicate route filters to ensure that this does not occur. For more information see CSCup04938.



CHAPTER 5

Documentation Update for Defects

- Command Line Interface Reference Guide, on page 29
- Security Guide, on page 29
- System Error Messages, on page 30
- Online Help for Cisco Unified Communications Manager, on page 33

Command Line Interface Reference Guide

utils dbreplication clusterreset

This documentation update resolves CSCvf93618.

The **utils dbreplication clusterreset** command is deprecated, instead run **utils dbreplication reset** command to repair replication.

```
admin:utils dbreplication clusterreset

******************************************************************************************
This command is deprecated, please use 'utils dbreplication reset' to repair replication!
******************************************************************************************

Executed command unsuccessfully
```

For more details on **utils dbreplication reset** command, see the “Utils Commands” chapter in the *Command Line Interface Guide for Cisco Unified Communications Solutions* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Security Guide

Certificates

This documentation update resolves CSCvg10775.

The following note is omitted from the “Security Overview” chapter in *Security Guide for Cisco Unified Communications Manager*.

Note The maximum supported size of certificate for DER or PEM is 4096 bits.

System Error Messages

Missing Device Type ENUM Values

This update is for CSCvg70867.

The *System Error Messages for Cisco Unified Communications Manager* file is missing the following ENUM definitions for the 78XX and 88xx phones.

Value	Device Type
508	Cisco IP Phone 7821
509	Cisco IP Phone 7841
510	Cisco IP Phone 7861
544	Cisco IP Phone 8831
568	Cisco IP Phone 8841
569	Cisco IP Phone 8851
570	Cisco IP Phone 8861
36665	Cisco IP Phone 7811
36669	Cisco IP Phone 8821
36670	Cisco IP Phone 8811
36677	Cisco IP Phone 8845
36678	Cisco IP Phone 8865
36686	Cisco IP Phone 8851NR
36701	Cisco IP Phone 8865NR

Missing Reason Codes for LastOutOfServiceInformation Alarms

This update is for CSCvd71818.

The *System Error Messages for Cisco Unified Communications* file is missing some ENUM values for the **Reason For Out Of Service** parameter within the **LastOutOfServiceInformation** alarm. Following is a complete list:

Reason Code	Description
10	TCPtimedOut - The TCP connection to the Cisco Unified Communication Manager experienced a timeout error
12	TCPucmResetConnection - The Cisco Unified Communication Manager reset the TCP connection
13	TCPucmAbortedConnection - The Cisco Unified Communication Manager aborted the TCP
14	TCPucmClosedConnection - The Cisco Unified Communication Manager closed the TCP connection
15	SCCPKeepAliveFailure - The device closed the connection due to a SCCP KeepAlive failure
16	TCPdeviceLostIPAddress - The connection closed due to the IP address being lost. This may be due to the DHCP Lease expiring or the detection of IP address duplication. Check that the DHCP Server is online and that no duplication has been reported by the DHCP Server
17	TCPdeviceLostIPAddress - The connection closed due to the IP address being lost. This may be due to the DHCP Lease expiring or the detection of IP address duplication. Check that the DHCP Server is online and that no duplication has been reported by the DHCP Server
18	TCPclosedConnectHighPriorityUcm - The device closed the TCP connection in order to reconnect to a higher priority Cisco Unified CM
20	TCPclosedUserInitiatedReset - The device closed the TCP connection due to a user initiated reset
22	TCPclosedUcmInitiatedReset - The device closed the TCP connection due to a reset command from the Cisco Unified CM
23	TCPclosedUcmInitiatedRestart - The device closed the TCP connection due to a restart command from the Cisco Unified CM
24	TCPClosedRegistrationReject - The device closed the TCP connection due to receiving a registration rejection from the Cisco Unified CM
25	RegistrationSuccessful - The device has initialized and is unaware of any previous connection to the Cisco Unified CM
26	TCPclosedVlanChange - The device closed the TCP connection due to reconfiguration of IP on a new Voice VLAN
27	Power Save Plus
30	Phone Wipe (wipe from CUCM)
31	Phone Lock (lock from CUCM)

Reason Code	Description
32	TCPclosedPowerSavePlus - The device closed the TCP connection in order to enter Power Save Plus mode
100	ConfigVersionMismatch - The device detected a version stamp mismatch during registration Cisco Unified CM
101	Config Version Stamp Mismatch
102	Softkeyfile Version Stamp Mismatch
103	Dial Plan Mismatch
104	TCPclosedApplyConfig - The device closed the TCP connection to restart triggered internally by the device to apply the configuration changes
105	TCPclosedDeviceRestart - The device closed the TCP connection due to a restart triggered internally by the device because device failed to download the configuration or dial plan file
106	TCPsecureConnectionFailed - The device failed to setup a secure TCP connection with Cisco Unified CM
107	TCPclosedDeviceReset - The device closed the TCP connection to set the inactive partition as active partition, then reset, and come up from the new active partition
108	VpnConnectionLost - The device could not register to Unified CM because VPN connectivity was lost 109 IP Address Changed
109	IP Address Changed
110	Application Requested Stop (service control notify to stop registering)
111	Application Requested Destroy
114	Last Time Crash
200	ClientApplicationClosed - The device was unregistered because the client application was closed
201	OsInStandbyMode - The device was unregistered because the OS was put in standby mode
202	OsInHibernateMode - The device was unregistered because the OS was put in hibernate mode
203	OsInShutdownMode - The device was unregistered because the OS was shut down
204	ClientApplicationAbort - The device was unregistered because the client application crashed
205	DeviceUnregNoCleanupTime - The device was unregistered in the previous session because the system did not allow sufficient time for cleanup

Reason Code	Description
206	DeviceUnregOnSwitchingToDeskphone - The device was unregistered because the client requested to switch from softphone to deskphone control
207	DeviceUnregOnSwitchingToSoftphone - The device is being registered because the client requested to switch from deskphone control to softphone
208	DeviceUnregOnNetworkChanged - The device is being unregistered because the client detected a change of network
209	DeviceUnregExceededRegCount - The device is being unregistered because the device has exceeded the maximum number of concurrent registrations
210	DeviceUnregExceededLoginCount - The device is being unregistered because the client has exceeded the maximum number of concurrent logons

Online Help for Cisco Unified Communications Manager

DHCP Subnet Setup Tips

This documentation update resolves CSCve07463.

The DHCP subnet setup tip is incorrect in the *Cisco Unified CM Administration Online Help*. The correct information for “DHCP Subnet Setup Tips” is as follows:

Changes to the server configuration do not take effect until you restart DHCP Monitor Service.

Insufficient Information About Opus Codec

This documentation update resolves CSCva48193.

The “System Menu” chapter in *Cisco Unified CM Administration Online Help* contains insufficient information about the **Opus Codec** field. The following note is omitted from the guide.

Note The Advertise G.722 Codec service parameter in the **Enterprise Parameters Configuration** window should be set to **Enabled** for the SIP devices to use Opus codec. For more information on enterprise parameters, see the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_5_1/sysConfig/CUCM_BK_SE5DAF88_00_cucm-system-configuration-guide-1151.html.

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 Time Schedule

This documentation update resolves CSCvd75418.

The Time Schedule Settings topic in the “Call Routing Menu” chapter of the *Cisco Unified CM Administration Online Help* contains insufficient information about the selected time period for a day. The following scenario is omitted from the guide:

Table 12: Time Schedule Settings

Field	**Description**
Time Period Information	

Field	Description
Selected Time Periods	**Scenario:** If multiple time periods are associated to a time schedule and the time periods does not overlap. However, overlap in a day, then the single day period takes precedence and other time periods for that day is ignored. Example 1: Three time periods are defined in the time schedule: Range of Days: Jan 1 - Jan 31: 09:00 - 18:00 Day of Week: Mon - Fri: 00:00 - 08:30 Day of Week: Mon - Fri: 18:30 - 24:00 In this case, even though the times are not overlapping, Range of Days is ignored for a call on Wednesday at 10:00. Example 2: Three time periods are defined in the time schedule: Single Day: Jan 3 2017 (Tues): 09:00 - 18:00 Day of Week: Mon - Fri: 00:00 - 08:30 Day of Week: Mon - Fri: 18:30 - 24:00 In this case, even though the times are not overlapping, Day of Week is ignored for a call on Jan 3 at 20:00. **Note** If Day of Year settings is configured, then the Day of Year settings is considered for the entire day (24 hours) and Day of Week settings, Range of Days settings for that particular day is ignored.

Insufficient Information on LDAP User Authentication

This documentation update resolves CSCvc30013.

The *LDAP Authentication Settings* in the *System Menu* chapter in *Cisco Unified CM Administration Online Help* contains insufficient information about LDAP User Authentication. The following note is omitted from the guide:

Note You can do LDAP User Authentication using the IP address or the hostname. When IP address is used while configuring the LDAP Authentication, LDAP configuration needs to be made the IP address using the command `utils ldap config ipaddr`. When hostname is used while configuring the LDAP Authentication, DNS needs to be configured to resolve that LDAP hostname.

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.

SIP Profile Field Descriptions Are Missing

The online help in Cisco Unified Communications Manager Releases 11.5(1)SU3 and SU4 contains an error in the SIP Profile Settings topic for the online help. This topic may be missing the SIP Profile field descriptions. If this is the case, refer to the following topic for the list of field descriptions.

SIP Profile Settings

The following table describes the available settings in the SIP Profile Configuration window.

Table 13: SIP Profile Settings

Field	Description
SIP Profile Information	
Name	Enter a name to identify the SIP profile; for example, SIP_7905. The value can include 1 to 50 characters, including alphanumeric characters, dot, dash, and underscores.
Description	Identifies the purpose of the SIP profile. For example, SIP for 7970. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Field	Description
Default MTP Telephony Event Payload Type	Specifies the default payload type for RFC2833 telephony event. See RFC 2833 for more information. Usually, the default value specifies the appropriate payload type. Ensure that you have a firm understanding of this parameter before changing it, as changes could result in DTMF tones not being received or generated. The default value specifies 101 with range from 96 to 127. The value of this parameter affects calls with the following conditions: • The call is an outgoing SIP call from Unified Communications Manager. • For the calling SIP trunk, the Media Termination Point Required check box is checked on the **SIP Trunk Configuration** window.
Early Offer for G.Clear Calls	The Early Offer for G.Clear Calls feature supports both standards-based G.Clear (CLEARMODE) and proprietary Cisco Session Description Protocols (SDP). To enable or disable Early Offer for G.Clear Calls, choose one of the following options: • Disabled • CLEARMODE • CCD • G.nX64 • X-CCD
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites	Specifies the maximum amount of bandwidth that is needed when all the media streams are used. There are three Session Level Bandwidth Modifiers: Transport Independent Application Specific (TIAS), Application Specific (AS), and Conference Total (CT). Select one of the following options to specify which Session Level Bandwidth Modifier to include in the SDP portion of SIP Early Offer or Reinvite requests. • TIAS and AS • TIAS only • AS only • CT only

Field	Description
User-Agent and Server header information	Indicates how Unified Communications Manager handles the User-Agent and Server header information in a SIP message. Choose one of the following three options: • Send Unified Communications Manager Version Information as User-Agent Header—For INVITE requests, the User-Agent header is included with the CM version header information. For responses, the Server header is omitted. Unified Communications Manager passes through any contact headers untouched. This is the default behavior. • Pass Through Received Information as Contact Header Parameters—If this option is selected, the User-Agent/Server header information is passed as Contact header parameters. The User-Agent/Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent/Server headers. • Pass Through Received Information as User-Agent and Server Header—If this option is selected, the User-Agent/Server header information is passed as User-Agent/Server headers. The User-Agent/Server header is derived from the received Contact header parameters, if present. Otherwise, they are taken from the received User-Agent/Server headers.

Field	Description
Dial String Interpretation	Determine if the SIP identity header is a directory number or directory URI. As directory numbers and directory URIs are saved in different database lookup tables, Unified Communications Manager examines the characters in the SIP identity header's user portion, which is the portion of the SIP address that is before the @ sign (for example, user@IP address or user@domain). To configure the Dial String Interpretation, choose one of the following options from the list: • Always treat all dial strings as URI addresses—Unified Communications Manager treats the address of incoming calls as if they were URI addresses. • Phone number consists of characters 0–9, A–D, *, and + (others that are treated as URI addresses)—Unified Communications Manager treats the incoming call as a directory number if all the characters in the user portion of the SIP identity header fall within this range. If the user portion of the address uses any characters that do not fall within this range, the address is treated as a URI. • Phone number consists of characters 0–9, *, and + (others that are treated as URI addresses)—Unified Communications Manager treats the incoming call as a directory number if all the characters in the user portion of the SIP identity header fall within this range. If the user portion of the address uses any characters that do not fall within this range, the address is treated as a URI. **Note** If the user=phone tag is present in the Request URI, Unified Communications Manager always treats the dial string as a number regardless of what option you choose for the Dial String Interpretation field.
Accept Audio Codec Preferences in Received Offer	Allows to select **On** to enable Unified Communications Manager to honor the preference of audio codecs in received offer and preserve it while processing. Select **Off** to enable Unified Communications Manager to ignore the preference of audio codecs in received offer and apply the locally configured Audio Codec Preference List. The default will select the service parameter configuration.

Field	Description
Require SDP Inactive Exchange for Mid-Call Media Change	Designates how Unified Communications Manager handles mid-call updates to codecs or connection information such as IP address or port numbers. If the check box is selcted, during mid-call codec or connection updates Unified Communications Manager sends an INVITE a=inactive SDP message to the endpoint to break the media exchange. This is required if an endpoint is not capable of reacting to changes in the codec or connection information without disconnecting the media. This applies only to audio and video streams within SIP-SIP calls. If the check box is unchecked, 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. **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.
Confidential Access Level Headers	Determines the inclusion of Confidential Access Level headers in INVITE and 200 OK messages. Valid values are as follows: • Disabled—CAL headers are not included. • Preferred—CAL headers are included and confidential-access-level tag is added in the Supported header. • Required— CAL headers are included and confidential-access-level tag is added in the Require and Proxy-Require headers.
SDP Transparency Profile	Allows you to choose one of the following options for SIP profile : • **None**—Choose this option for Unified Communications Manager to filter out known SDP attributes only. By default, this option is selected. • **Pass all unknown SDP attributes**—Choose this option for media adaptation and resilience (MARI). To ensure that the session level MARI attributes pass the unknown attributes through Unified Communications Manager, choose this value on the SIP profile, which is associated with both the originating device and the terminating device.

Field	Description
Redirect by Application	Checking this check box and configuring this SIP Profile on the SIP trunk allows the Unified Communications Manager administrator to: • Apply a specific calling search space to redirected contacts that are received in the 3xx response. • Apply digit analysis to the redirected contacts to make sure that the call get routed correctly. • Prevent DOS attack by limiting the number of redirection (recursive redirection) that a service parameter can set. • Allow other features to be invoked while the redirection is taking place. Getting redirected to a restricted phone number (such as an international number) means that handling redirection at the stack level causes the call to be routed instead of being blocked. This behavior occurs if the Redirect by Application check box is unchecked.
Disable Early Media on 180	By default, Unified Communications Manager signals the calling phone to play local ringback if SDP is not received in the 180 response. If SDP is included in the 180 response, instead of playing ringback locally, Unified Communications Manager connects media, and the calling phone plays whatever the called device is sending (such as ringback or busy signal). If you do not receive ringback, the device to which you are connecting may be including SDP in the 180 response, but it is not sending any media before the 200OK response. In this case, check this check box to play local ringback on the calling phone and connect the media upon receipt of the 200OK response **Note** Even though the phone that is receiving ringback is the calling phone, you need the configuration on the called device profile because it determines the behavior.
Outgoing T.38 INVITE Include Audio mline	Allows the system to accept a signal from Microsoft Exchange that causes it to switch the call from audio to T.38 fax. To use this feature, you must also configure a SIP trunk with this SIP profile. For more information, see Chapter 68, Trunk "Configuration." **Note** The parameter applies to SIP trunks only, not phones that are running SIP or other endpoints.
Offer valid IP and Send/Receive mode only for T.38 Fax Relay	If this checkbox is checked, this SIP profile on the trunk allows you to send a fax offer with a valid IP address and with Send Receive SDP mode. If this checkbox is not checked, this SIP profile on the trunk allows you to send a fax offer with a null IP address and with Send Receive SDP mode. This parameter applies only to trunks, not phones that are running SIP or other endpoints. It applies only for T38 fax relay and, by default, this checkbox is unchecked.

Field	Description
Enable ANAT	Allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media. When you check both the Enable ANAT and the MTP Required check boxes, Unified Communications Manager inserts a dual-stack MTP and sends out an offer with two m-lines, one for IPv4 and another for IPv6. If a dual-stack MTP cannot be allocated, Unified Communications Manager sends an INVITE without SDP. When you check the Enable ANAT check box and the Media Termination Point Required check box is unchecked, Unified Communications Manager sends an INVITE without SDP. When the Enable ANAT and Media Termination Point Required check boxes display as unchecked (or when an MTP cannot be allocated), Unified Communications Manager sends an INVITE without SDP. When you uncheck the Enable ANAT check box but you check the Media Termination Point Required check box, consider the information, which assumes that an MTP can be allocated: • Unified Communications Manager sends an IPv4 address in the SDP for SIP trunks with an IP Addressing Mode of IPv4 Only. • Unified Communications Manager sends an IPv6 address in the SDP for SIP trunks with an IP Addressing Mode of IPv6 Only. • For dual-stack SIP trunks, Unified Communications Manager determines which IP address type to send in the SDP based on the configuration for the IP Addressing Mode Preference for Media enterprise parameter. • For dual-stack SIP trunks, Unified Communications Manager determines which IP address type to send in the SDP based on the configuration for the IP Addressing Mode Preference for Media enterprise parameter.
Require SDP Inactive Exchange for Mid-Call Media Change	Designates how Unified Communications Manager handles mid-call updates to codecs or connection information such as IP address or port numbers. If the box is checked, during mid-call codec or connection updates Unified Communications Manager sends an INVITE a=inactive SDP message to the endpoint to break the media exchange. This is required if an endpoint is not capable of reacting to changes in the codec or connection information without disconnecting the media. This applies only to audio and video streams within SIP-SIP calls. **Note** For early offer enabled SIP trunks, this parameter will be overridden by the Send send-receive SDP in mid-call INVITE parameter. If the box is unchecked, 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.

Field	Description
Use Fully Qualified Domain Name in SIP Requests	Enables Unified Communications Manager to relay an alphanumeric hostname of a caller by passing it through to the called device or outbound trunk as a part of the SIP header information. • If the box is unchecked, the IP address for Unified Communications Manager will be passed to the line device or outbound trunk instead of the user's hostname. This is the default behavior. • If the box is checked, Unified Communications Manager will relay an alphanumeric hostname of a caller by passing it through to the called endpoint as a part of the SIP header information. This enables the called endpoint to return the call using the received or missed call list. If the call is originating from a line device on the Unified Communications Manager cluster, and is being routed on a SIP trunk then the configured Organizational Top-Level Domain (e.g., cisco.com) will be used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID. If the call is originating from a trunk on Unified Communications Manager and is being routed on a SIP trunk then: • If the inbound call provides a host or domain in the caller's information, the outbound SIP trunk messaging will preserve the hostname in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID • If the inbound call does not provide a host or domain in the caller's information, the configured Organizational Top-Level Domain will be used in the Identity headers, such as From, Remote-Party-ID, and P-Asserted-ID
Assured Services SIP conformance	Specifies to check this box for third-party AS-SIP endpoints as well as AS-SIP trunks to ensure proper Assured Service behavior. This setting provides specific Assured Service behavior that affects services such as Conference factory and SRTP.
Enable External QoS	Specifies to check this box to configure this SIP Profile for external QoS support. With this feature enabled, you can use an APIC-EM Controller to manage QoS for SIP media flows for devices that use this SIP Profile. The default value is unchecked. **Note** This check box appears only if the **External QoS Enable** service parameter is set to **True**.
Parameters Used in Phone	
Timer Invite Expires (seconds)	Sspecifies the time, in seconds, after which a SIP INVITE expires. The Expires header uses this value. Valid values include any positive number; 180 specifies the default.
Timer Register Delta (seconds)	Intended to be used by SIP endpoints only. The endpoint receives this value via a tftp config file. The end point reregisters Timer Register Delta seconds before the registration period ends. The registration period gets determined by the value of the SIP Station KeepAlive Interval service parameter. Valid values for Timer Register Delta range from 32767 to 0. The default value is 5.

Field	Description
Timer Register Expires (seconds)	Intended to be used by SIP endpoints only. The SIP endpoint receives the value via a tftp config file. This field specifies the value that the phone that is running SIP sends in the Expires header of the REGISTER message. Valid values include any positive number; however, 3600 (1 hour) specifies the default value. If the endpoint sends a shorter Expires value than the value of the SIP Station Keepalive Interval service parameter, Unified Communications Manager responds with a 423 "Interval Too Brief". If the endpoint sends an Expires value that is greater than the SIP Station Keepalive Interval service parameter value, Unified Communications Manager responds with a 200 OK that includes the Keepalive Interval value for Expires. **Note** For mobile phones that are running SIP, Unified Communications Manager uses the value in this field instead of the value that the SIP Station KeepAlive Interval service parameter specifies to determine the registration period. **Note** For TCP connections, the value for the Timer Register Expires field must be lower than the value for the SIP TCP Unused Connection service parameter.
Timer T1 (msec)	Specifies the lowest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number. Default specifies 500.
Timer T2 (msec)	Specifies the highest value, in milliseconds, of the retransmission timer for SIP messages. Valid values include any positive number. Default specifies 4000.
Retry INVITE	Specifies the maximum number of times that an INVITE request gets retransmitted. Valid values include any positive number. Default specifies 6.
Retry Non-INVITE	Specifies the maximum number of times that a SIP message other than an INVITE request gets retransmitted. Valid values include any positive number. Default specifies 10.
Media Port Ranges	Specifies to click the radio button that corresponds to how you want to manage QoS for audio and video calls for devices that are associated to this SIP Profile • **Common Port Range for Audio and Video**—Choose this option if you want to use a common port range that can handles both the audio and video media stream. • **Separate Port Ranges for Audio and Video**—Choose this option if you want to set up a distinct port range for the audio stream and a distinct port range for the video stream.
Start Media Port	Designates the start real-time protocol (RTP) port for media. Media port ranges from 2048 to 65535. Default specifies 16384. This field appears when you select **Common Port Range for Audio and Video** as the **Media Port Range**.

Field	Description
Stop Media Port	Designates the stop real-time protocol (RTP) port for media. Media port ranges from 2048 to 65535. Default specifies 32766. This field appears when you select **Common Port Range for Audio and Video** for the **Media Port Range**.
Start Audio Port	Allows you to create a port range for audio by entering the start of the port range. For example, 16384. The audio port range cannot overlap the video port range. This field appears when you select **Separate Port Ranges for Audio and Video** for the **Media Port Range**.
Stop Audio Port	Allows you to enter the ending of the port range for audio calls. The audio port range must not overlap the video port range. For example, 32766. This field appears when you select **Separate Port Ranges for Audio and Video** for the **Media Port Range**.
Start Video Port	Allows you to create a port range for the video stream of a video call by entering the beginning of the port range. For example, 32767. The video port range cannot overlap with the audio port range. This field appears when you select **Separate Port Ranges for Audio and Video** for the **Media Port Range**.
Stop Video Port	Allows you to enter the ending of the port range for audio calls. The audio port range must not overlap the video port range. This field appears when you select **Separate Port Ranges for Audio and Video** for the **Media Port Range**.
DSCP for Audio Calls	Allows you to select the value that you want to assign as the DSCP value for audio-only calls. The Default Option is to use the value of the DSCP for Audio Calls service parameter.
DSCP for Video Calls	Allows you to select the value that you want to assign as the DSCP value for video calls. The Default Option is to use the value of the DSCP for Video Calls service parameter.
DSCP for Audio Portion of Video Calls	Allows you to select the value that you want to assign as the DSCP value for audio portion of a video call. The default option is to use the value that is configured in the DSCP for Audio Portion of Video Calls service parameter. **Note** If you choose a different DSCP value for audio portion of video calls than you configured for DSCP Video Calls, it could mean that the audio and video streams within a single video call could have different DSCP markings and different QoS policy control, which could result in lip sync issues that result from network bandwidth issues.
DSCP for TelePresence Calls	Allows you to select the value that you want to assign as the DSCP value for TelePresence calls. The default option is to use the value of the DSCP for TelePresence Calls service parameter.

Field	Description
DSCP for Audio Portion of TelePresence Calls	Allows you to select the value that you want to assign as the DSCP value for the audio portion of TelePresence calls. The default option is to use the value of the DSCP for TelePresence Calls service parameter.
Call Pickup URI	Provides a unique address that the phone that is running SIP sends to Unified Communications Manager to invoke the call pickup feature.
Call Pickup Group Other URI	Provides a unique address that the phone that is running SIP sends to Unified Communications Manager to invoke the call pickup group other feature.
Call Pickup Group URI	Provides a unique address that the phone that is running SIP sends to Unified Communications Manager to invoke the call pickup group feature.
Meet Me Service URI	Provides a unique address that the phone that is running SIP sends to Unified Communications Manager to invoke the meet me conference feature.
User Info	Configures the user= parameter in the REGISTER message. Valid values follow: • none—No value gets inserted. • phone—The value user=phone gets inserted in the To, From, and Contact Headers for REGISTER. • ip—The value user=ip gets inserted in the To, From, and Contact Headers for REGISTER.
DTMF DB Level	Specifies in-band DTMF digit tone level. Valid values follow: • 1 to 6 dB below nominal • 2 to 3 dB below nominal • 3 nominal • 4 to 3 dB above nominal • 5 to 6 dB above nominal
Call Hold Ring Back	Indicates the call on hold status. For example, if you have a call on hold and are talking on another call, when you hang up the call, this parameter causes the phone to ring to let you know that you still have another party on hold. Valid values follow: • Off permanently and cannot be turned on and off locally by using the user interface. • On permanently and cannot be turned on and off locally by using the user interface.

Field	Description
Anonymous Call Block	Configures anonymous call block. Valid values follow: • Off—Disabled permanently and cannot be turned on and off locally by using the user interface. • On—Enabled permanently and cannot be turned on and off locally by using the user interface.
Caller ID Blocking	Configures caller ID blocking. When blocking is enabled, the phone blocks its own number or e-mail address from phones that have caller identification enabled. Valid values follow: • Off—Disabled permanently and cannot be turned on and off locally by using the user interface. • On—Enabled permanently and cannot be turned on and off locally by using the user interface.
Do Not Disturb Control	Sets the Do Not Disturb (DND) feature. Valid values follow: • User—The dndControl parameter for the phone should specify 0. • Admin—The dndControl parameter for the phone should specify 2.
Telnet Level for 7940 and 7960	Unified IP Phones 7940 and 7960 do not support ssh for login access or HTTP that is used to collect logs; however, these phones support Telnet, which lets the user control the phone, collect debugs, and look at configuration settings. This field controls the telnet_level configuration parameter with the following possible values: • Disabled (no access) • Limited (some access but cannot run privileged commands) • Enabled (full access)
Resource Priority Namespace	Enables the admin to select one of the cluster's defined Resource Priority Namespace network domains for assignment to a line via its SIP Profile.
Timer Keep Alive Expires (seconds)	Specifies the interval between keepalive messages that are sent to the backup Unified Communications Manager to ensure that it is available in the event that a failover is required. Unified Communications Manager requires a keepalive mechanism to support redundancy.
Timer Subscribe Expires (seconds)	Specifies the time, in seconds, after which a subscription expires. This value gets inserted into the Expires header field. Valid values include any positive number; however, 120 specifies the default value.

Field	Description
Timer Subscribe Delta (seconds)	Allows you to use this parameter in conjunction with the Timer Subscribe Expires setting. The phone resubscribes Timer Subscribe Delta seconds before the subscription period ends, as governed by Timer Subscribe Expires. Valid values range from 3 to 15. Default specifies 5.
Maximum Redirections	Allows you to use this configuration variable to determine the maximum number of times that the phone allows a call to be redirected before dropping the call. Default specifies 70 redirections.
Off Hook to First Digit Timer (microseconds)	Specifies the time in microseconds that passes when the phone goes off hook and the first digit timer gets set. The value ranges from 0 - 150,000 microseconds. Default specifies 15,000 microseconds.
Call Forward URI	Provides a unique address that the phone that is running SIP sends to Unified Communications Manager to invoke the call forward feature.
Abbreviated Dial URI	Provides a unique address that the phone that is running SIP sends to Unified Communications Manager to invoke the abbreviated dial feature. Speed dials that are not associated with a line key (abbreviated dial indices) do not download to the phone. The phone uses the feature indication mechanism (INVITE with Call-Info header) to indicate when an abbreviated dial number has been entered. The request URI contains the abbreviated dial digits (for example, 14), and the Call-Info header indicates the abbreviated dial feature. Unified Communications Manager translates the abbreviated dial digits into the configured digit string and extend the call with that string. If no digit string has been configured for the abbreviated dial digits, a 404 Not Found response gets returned to the phone.
Conference Join Enabled	Determines whether the Unified IP Phones 7940 or 7960, when the conference initiator that is using that phone hangs up, should attempt to join the remaining conference attendees. Check the check box if you want to join the remaining conference attendees; leave it unchecked if you do not want to join the remaining conference attendees. **Note** This check box applies to the Unified IP Phones 7941/61/70/71/11 when they are in SRST mode only.
RFC 2543 Hold	Enables setting connection address to 0.0.0.0 per RFC2543 when call hold is signaled to Unified Communications Manager. This allows backward compatibility with endpoints that do not support RFC3264.
Semi Attended Transfer	Determines whether the Unified IP Phones 7940 and 7960 caller can transfer the second leg of an attended transfer while the call is ringing. Check the check box if you want semi-attended transfer enabled; leave it unchecked if you want semi-attended transfer disabled. **Note** This check box applies to the Unified IP Phones 7941/61/70/71/11 when they are in SRST mode only.

Field	Description
Enable VAD	Enables Voice Activation Detection (VAD). When VAD is enabled, media is not transmitted until the voice is detected.
Stutter Message Waiting	Enables stutter dial tone when the phone goes off hook and a message is waiting; leave unchecked if you do not want a stutter dial tone when a message is waiting. This setting supports Unified IP Phones 7960 and 7940 that run SIP.
MLPP User Authorization	Enable MLPP User Authorization. MLPP User Authorization requires the phone to send in an MLPP username and password.
Normalization Script	
Normalization Script	Alows you to choose the script that you want to apply to this SIP profile. To import another script, go to the SIP Normalization Script Configuration window (**Device** > **Device Settings** > **SIP Normalization Script**), and import a new script file. **Caution** A normalization script in the SIP profile is only valid for non-trunk devices.
Parameter Name/Parameter Value	Optionally, enter parameter names and parameter values. Valid values include all characters except equals signs (=), semi-colons (;), and non-printable characters, such as tabs. You can enter a parameter name with no value. To add another parameter line, click the + (plus) button. To delete a parameter line, click the - (minus) button. **Note** You must choose a script from the Normalization Script list before you can enter parameter names and values.
Enable Trace	Enables tracing within the script or uncheck this check box to disable tracing. When checked, the trace.output API provided to the Lua scripter produces SDI trace **Note** We recommend that you only enable tracing while debugging a script. Tracing impacts performance and should not be enabled under normal operating conditions.
Incoming Requests FROM URI Settings	
Caller ID DN	Allows you to enter the pattern that you want to use for calling line ID, from 0 to 24 digits. For example, in North America: • 555XXXX = Variable calling line ID, where X equals an extension number. The CO appends the number with the area code if you do not specify it. • 55000 = Fixed calling line ID, where you want the Corporate number to be sent instead of the exact extension from which the call is placed. The CO appends the number with the area code if you do not specify it. You can also enter the international escape character +.

Field	Description
Caller Name	Allows you to enter a caller name to override the caller name that is received from the originating SIP Device.
Trunk Specific Configuration	
Reroute Incoming Request to new Trunk based on	Unified Communications Manager only accepts calls from the SIP device whose IP address matches the destination address of the configured SIP trunk. In addition, the port on which the SIP message arrives must match the one that is configured on the SIP trunk. After Unified Communications Manager accepts the call, Unified Communications Manager uses the configuration for this setting to determine whether the call should get rerouted to another trunk. Select the method that Unified Communications Manager uses to identify the SIP trunk where the call gets rerouted: • Never—If the SIP trunk matches the IP address of the originating device, choose this option, which equals the default setting. Unified Communications Manager, which identifies the trunk by using the source IP address of the incoming packet and the signaling port number, does not route the call to a different (new) SIP trunk. The call occurs on the SIP trunk on which the call arrived. • Contact Info Header—If the SIP trunk uses a SIP proxy, choose this option. Unified Communications Manager parses the contact header in the incoming request and uses the IP address or domain name and signaling port number that is specified in the header to reroute the call to the SIP trunk that uses the IP address and port. If no SIP trunk is identified, the call occurs on the trunk on which the call arrived. • Call-Info Header with purpose=x-cisco-origIP—If the SIP trunk uses a Customer Voice Portal (CVP) or a Back-to-Back User Agent (B2BUA), choose this option. When the incoming request is received, Unified Communications Manager parses the Call-Info header, looks for the parameter, purpose=x-cisco-origIP, and uses the IP address or domain name and the signaling port number that is specified in the header to reroute the call to the SIP trunk that uses the IP address and port. If the parameter does not exist in the header or no SIP trunk is identified, the call occurs on the SIP trunk on which the call arrived. **Tip** This setting does not work for SIP trunks that are connected to a Unified Presence proxy server or SIP trunks that are connected to originating gateways in different Unified CM groups.
Resource Priority Namespace List	Allows you to select a configured Resource Priority Namespace list. Configure the lists in the Resource Priority Namespace List menu that is accessed from **System** > **MLPP** > **Namespace**.

Field	Description
SIP Rel1XX Options	Configures SIP Rel1XX, which determines whether all SIP provisional responses (other than 100 Trying messages) get sent reliably to the remote SIP endpoint. Valid values follow: • Disabled—Disables SIP Rel1XX. • Send PRACK if 1XX contains SDP—Acknowledges a 1XX message with PRACK, only if the 1XX message contains SDP. • Send PRACK for all 1XX messages—Acknowledges all1XX messages with PRACK. **Note** You need not configure the above field if **Connect Inbound Call before Playing Queuing Announcement** checkbox is checked in the Trunk Specific Configuration.
Session Refresh Method	Session Timer with Update: The session refresh timer allows for periodic refresh of SIP sessions, which allows the Unified Communications Manager and remote agents to determine whether the SIP session is still active. Prior to Release 10.01, when the Unified Communications Manager received a refresh command, it supported receiving either Invite or Update SIP requests to refresh the session. When the Unified Communications Manager initiated a refresh, it supported sending only Invite SIP requests to refresh the session. With Release 10.01, this feature extends the refresh capability so that Unified Communications Manager can send both Update and Invite requests. Specify whether Invite or Update should be used as the Session Refresh Method. **Invite** (default): **Note** Sending a mid-call Invite request requires that an offer SDP be specified in the request. This means that the far end must send an answer SDP in the Invite response. **Update**: Unified Communications Manager sends a SIP Update request, if support for the Update method is specified by the far end of the SIP session either in the Supported or Require headers. When sending the Update request, the Unified Communications Manager includes an SDP. This simplifies the session refresh since no SDP offer/answer exchange is required. **Note** If the Update method is not supported by the far end of the SIP session, the Unified Communications Manager continues to use the Invite method for session refresh.

Field	Description
Early Offer support for voice and video calls	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. 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. Unified Communications Manager sends the MTP IP address and port with a single codec in the SDP in the initial INVITE. Select one of the following three options: • Disabled (Default value) - Disables Early Offer; no SDP will be included in the initial INVITE for outbound calls. • Best Effort (no MTP inserted) • Provide Early Offer for the outbound call only when caller side's media port, IP and codec information is available. • Provide Delayed Offer for the outbound call when caller side's media port, IP and codec information is not available. No MTP is inserted to provide Early Offer in this case. • 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.
Video Call Traffic Class	Determines the type of video endpoint or trunk that the SIP Profile is associated with. From the list, select one of the following three options • Immersive—High-definition immersive video. • Desktop—Standard desktop video. • Mixed—A mix of immersive and desktop video. Unified Communications Manager Locations Call Admission Control (CAC) reserves bandwidth from two Locations video bandwidth pools, "Video Bandwidth" and/or "Immersive Bandwidth", depending on the type of call determined by the Video Call Traffic Class.
Calling Line Identification Presentation	Select **Strict From URI presentation Only** to select the network provided identity. Select **Strict Identity Headers presentation Only** to select the user provided identity.

Field	Description
Deliver Conference Bridge Identifier	Allows the SIP trunk to pass the b-number that identifies the conference bridge across the trunk instead of changing the b-number to the null value. The terminating side does not require that this field be enabled. Checking this check box is not required for Open Recording Architecture (ORA) SIP header enhancements to the Recording feature to work. Enabling this check box allows the recorder to coordinate recording sessions where the parties are participating in a conference.
Early Offer support for voice and video calls (insert MTP if needed)	Allows you want to create a trunk that supports early offer. Early Offer configurations on SIP profile apply to SIP trunk calls. These configurations do not affect SIP line side calls. If this profile is shared between a trunk and a line, only the SIP trunk that uses the profile provides early offer. **Note** When checked, the Media Termination Required check box on the Trunk Configuration window overrides the early offer configuration on the associated SIP profile. The Unified Communications Manager sends the MTP IP address and port with a single codec in the SDP in the initial INVITE.
Send send-receive SDP in mid-call INVITE	Allows you to prevent Unified Communications Manager from sending an INVITE a=inactive SDP message during call hold or media break during supplementary services. **Note** This check box applies only to early offer or best early offer enabled SIP trunks and has no impact on SIP line calls. When you enable Send send-receive SDP in mid-call INVITE for an early offer or best early offer SIP trunk in tandem mode, Unified Communications Manager inserts MTP to provide sendrecv SDP when a SIP device sends offer SDP with a=inactive or sendonly or recvonly in audio media line. In tandem mode, Unified Communications Manager depends on the SIP devices to initiate reestablishment of media path by sending either a delayed INVITE or mid-call INVITE with send-recv SDP. 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 overrides the Require SDP Inactive Exchange for Mid-Call Media Change, so Unified Communications Manager does not send an INVITE with a=inactive SDP in mid-call codec updates. For SIP line side calls, the Require SDP Inactive Exchange for Mid-Call Media Change check box applies when enabled. **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**) to True.

Field	Description
Allow Presentation Sharing using BFCP	Allows the supported SIP endpoints to use the Binary Floor Control Protocol to enable presentation sharing. The use of BFCP creates an additional media stream in addition to the existing audio and video streams. This additional stream is used to stream a presentation, such as a PowerPoint presentation from someone's laptop, into a SIP videophone. If the box is unchecked, Unified Communications Manager rejects BFCP offers from devices associated with the SIP profile by setting the BFCP application line and associated media line ports to 0 in the answering SDP message. This is the default behavior. **Note** BFCP is only supported on SIP networks. BFCP must be enabled on all SIP trunks, lines, and endpoints for presentation sharing to work. BFCP is not supported if the SIP line or SIP trunk uses MTP, RSVP, TRP or Transcoder.
Allow iX Application Media	Enables support for iX media channel.
Allow Passthrough of Configured Line Device Caller Information	Allows passthrough of configured line device caller information from the SIP trunk.
Reject Anonymous Incoming Calls	Allows to reject anonymous incoming calls.
Reject Anonymous Outgoing Calls	Allows to reject anonymous outgoing calls.

Field	Description
Allow multiple codecs in answer SDP	Applies when incoming SIP signals do not indicate support for multiple codec negotiation and Unified Communications Manager can finalize the negotiated codec. When this check box is checked, the endpoint behind the trunk is capable of handling multiple codecs in the answer SDP. For example, an endpoint that supports multiple codec negotiation calls the SIP trunk and Unified Communications Manager sends a Delay Offer request to a trunk. The endpoint behind the trunk returns all support codecs without the Contact header to indicate the support of multiple codec negotiation. In this case, Unified Communications Manager identifies the trunk as capable of multiple codec negotiation and sends SIP response messages back to both endpoints with multiple common codecs. When this check box is unchecked, Unified Communications Manager identifies the endpoint behind the trunk as incapable of multiple codec negotiation, unless indicated otherwise by SIP contact header URI. Unified Communications Manager continues the call with single codec negotiation. 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 Unified Communications Manager systems.
Send ILS Learned Destination Route String	Allows the calls that Unified Communications Manager routes to a learned directory URI, learned number, or learned pattern, Unified Communications Manager adds the *x-cisco-dest-route-string* header to outgoing SIP INVITE and SUBSCRIBE messages and inserts the destination route string into the header. When this check box is unchecked, Unified Communications Manager does not add the *x-cisco-dest-route-string* header to any SIP messages. The *x-cisco-dest-route-string* header allows Unified Communications Manager to route calls across a Unified Border Element.
Connect Inbound Call before Playing Queuing Announcement	Allows you to send the carrier a CONNECT message before playing the hunt group announcements. You should enable this feature if the carrier trunk does not support in-band call status updates or if external callers report that they are unable to hear hunt group announcements.
SIP OPTIONS Ping	

Field	Description
Enable OPTIONS Ping to monitor destination status for Trunks with service type "None (Default)"	Allows you to enable the SIP OPTIONS feature. SIP OPTIONS are requests to the configured destination address on the SIP trunk. If the remote SIP device fails to respond or sends back a SIP error response such as 503 Service Unavailable or 408 Timeout, Unified Communications Manager reroute the calls using other trunks or using a different address. If this check box is unchecked, the SIP trunk does not track the status of SIP trunk destinations. If this check box is checked, you can change the ping timer to a smaller value if required.
Ping Interval for In-service and Partially In-service Trunks (seconds)	Configures the time duration between SIP OPTIONS requests when the remote peer is responding and the trunk is marked as In Service. If at least one IP address is available, the trunk is In Service; if all IP addresses are unavailable, the trunk is Out of Service. The default value specifies 60 seconds. Valid values range from 5 to 600 seconds.
Ping Interval for Out-of-service SIP Trunks (seconds)	Configures the time duration between SIP OPTIONS requests when the remote peer is not responding and the trunk is marked as Out of Service. The remote peer may be marked as Out of Service if it fails to respond to OPTIONS, if it sends 503 or 408 responses, or if the Transport Control Protocol (TCP) connection cannot be established. If at least one IP address is available, the trunk is In Service; if all IP addresses are unavailable, the trunk is Out of Service. The default value specifies 120 seconds. Valid values range from 5 to 600 seconds.
Ping Retry Timer (milliseconds)	Specifies the maximum waiting time before retransmitting the OPTIONS request. Valid values range from 100 to 1000 milliseconds. The default value specifies 500 milliseconds.
Ping Retry Count	Specifies the number of times that Unified Communications Manager resends the OPTIONS request to the remote peer. After the configured retry attempts are used, the destination is considered to have failed. To obtain faster failure detection, keep the retry count low. Valid values range from 1 to 10. The default value specifies 6.

CHAPTER 6

Configure Centralized Deployment

- Centralized Deployment Overview, on page 57
- Centralized Deployment Prerequisites, on page 61
- Centralized Deployment Configuration Task Flow, on page 62
- Centralized Deployment Field Descriptions, on page 74
- Centralized Deployment Interactions and Restrictions, on page 74

Centralized Deployment Overview

The IM and Presence centralized deployment allows you to deploy your IM and Presence deployment and your telephony deployment in separate clusters. The central IM and Presence cluster handles IM and Presence for the enterprise, while the remote Cisco Unified Communications Manager telephony cluster handles voice and video calls for the enterprise.

The Centralized Deployment option provides the following benefits when compared to standard deployments:

- The Centralized Deployment option does not require a 1x1 ratio of telephony clusters to IM and Presence Service clusters–you can scale your IM and Presence deployment and your telephony deployment separately, to the unique needs of each.
- Full mesh topology is not required for the IM and Presence Service
- Version independent from telephony–your IM and Presence central cluster can be running a different version than your Cisco Unified Communications Manager telephony clusters.
- Can manage IM and Presence upgrades and settings from the central cluster.
- Lower cost option, particularly for large deployments with many Cisco Unified Communications Manager clusters
- Easy XMPP Federation with third parties.
- Supports calendar integration with Microsoft Outlook. For configuration details, refer to the document *Microsoft Outlook Calendar Integration for the IM and Presence Service*.

OVA Requirements

For Centralized Deployments, we recommend the 25,000 user IM and Presence OVA with a minimum OVA of 15,000 users. The 15,000 user OVA can grow to 25,000 users. With a 25K OVA template, and a six-node cluster with High Availability enabled, the IM and Presence Service central deployment supports up to 75,000 clients. To support 75K users with 25K OVA, default trace level for XCP router needs to be changed from **Info** to **Error**. For the Unified Communications Manager publisher node in the central cluster, the following requirements apply:

- A 25,000 IM and Presence OVA (maximum 75,000 users) can be deployed with a 10,000 user OVA installed on the central cluster's Unified Communications Manager publisher node
- A 15,000 IM and Presence OVA (maximum 45,000 users) can be deployed with a 7,500 user OVA installed on the central cluster's Unified Communications Manager publisher node

Note If you plan to enable Multiple Device Messaging, measure deployments by the number of clients instead of the number of users as each user may have multiple Jabber clients. For example, if you have 25,000 users, and each user has two Jabber clients, your deployment requires the capacity of 50,000 users.

Interclustering for Centralized Deployment

Interclustering is supported between two centralized clusters. Intercluster peering is tested with one cluster with 25K (with 25K OVA) and another with 15K (with 15K OVA) devices and no performance issues were observed.

Centralized Deployment Setup vs Standard (Decentralized) Deployments

The following table discusses some of the differences in setting up an IM and Presence Centralized Cluster Deployment as opposed to standard deployments of the IM and Presence Service.

Setup Phase	Differences with Standard Deployments
Installation Phase	The installation process for an IM and Presence central deployment is the same as for the standard deployment. However, with central deployments, the IM and Presence central cluster is installed separatelyfrom your telephony cluster, and may be located on separate hardware servers. Depending on how you plan your topology, the IM and Presence central cluster may be installed on separate physical hardware from your telephony cluster. For the IM and Presence central cluster, you must still install Cisco Unified Communications Manager and then install the IM and Presence Service on the same servers. However, the Cisco Unified Communications Manager instance of the IM and Presence central cluster is for database and user provisioning primarily, and does not handle voice or video calls.

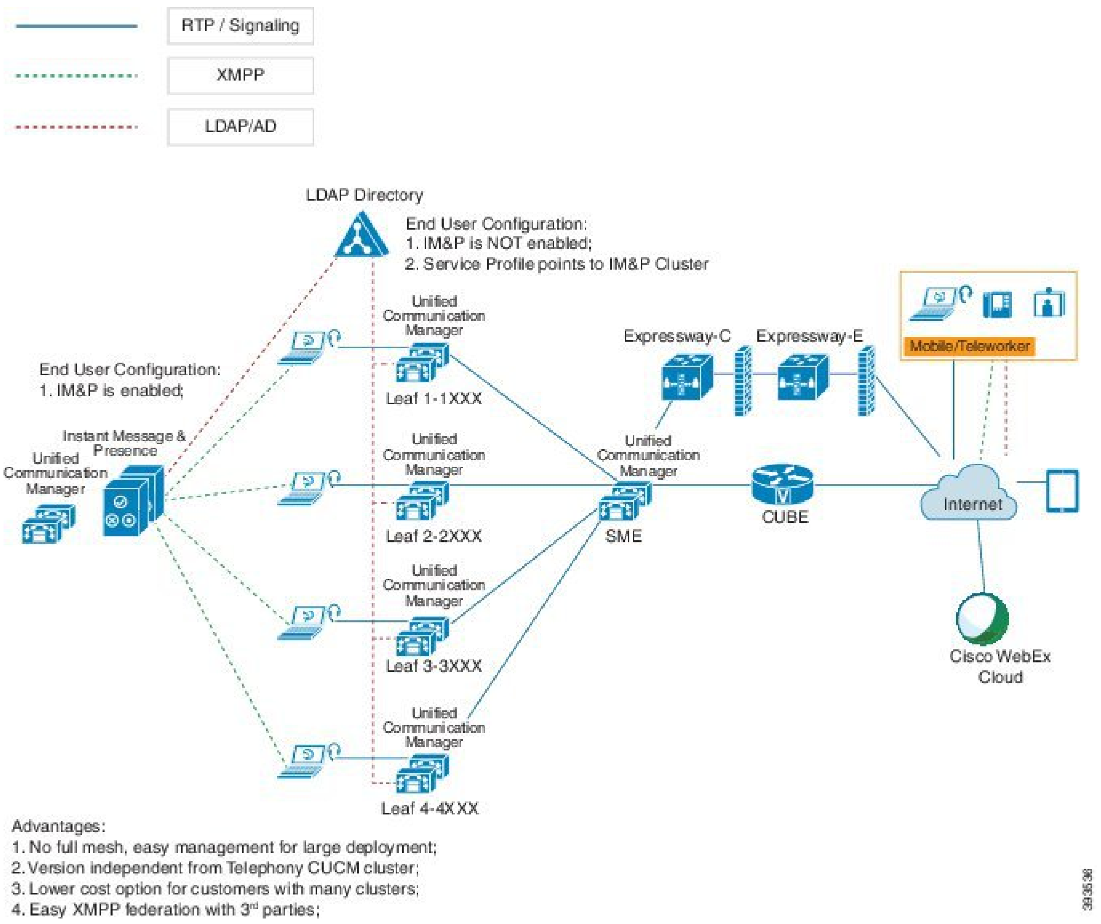
Setup Phase	Differences with Standard Deployments
Configuration Phase	Compared to standard (decentralized) deployments, the following extra configurations are required to set up the IM and Presence Service Central Deployment: • Users must be synced into both the telephony cluster and the IM and Presence Service central cluster so that they exist in both databases. • In your telephony clusters, end users should not be enabled for IM and Presence. • In your telephony clusters, the Service Profile must include the IM and Presence Service and must point to the IM and Presence central cluster. • In the IM and Presence central cluster, users must be enabled for the IM and Presence Service. • In the IM and Presence central cluster's database publisher node, add your remote Cisco Unified Communications Manager telephony cluster peers. The following configurations, which are used with Standard Deployments of the IM and Presence Service, but are not required with Central Deployments: • A Presence Gateway is not required. • A SIP Publish trunk is not required. • A Service Profile is not required on the IM and Presence central cluster—the Service Profile is configured on the telephony cluster to which the central cluster connects

Centralized Cluster Deployment Architecture

The following diagram highlights the cluster architecture for this deployment option. Cisco Jabber clients connect to multiple Cisco Unified Communications Manager clusters for voice and video calling. In this example, the Cisco Unified Communications Manager telephony clusters are leaf clusters in a Session Management Edition deployment. For Rich Presence, Cisco Jabber clients connect to the IM and Presence Service central cluster. The IM and Presence central cluster manages instant messaging and presence for the Jabber clients.

Note Your IM and Presence cluster still contains an instance for Cisco Unified Communications Manager. However, this instance is for handling shared features such as database and user provisioning–it does not handle telephony.

Figure 1: IM and Presence Service Centralized Cluster Architecture



End User Configuration:
1. IM&P is NOT enabled;
2. Service Profile points to IM&P Cluster

End User Configuration:
1. IM&P is enabled;

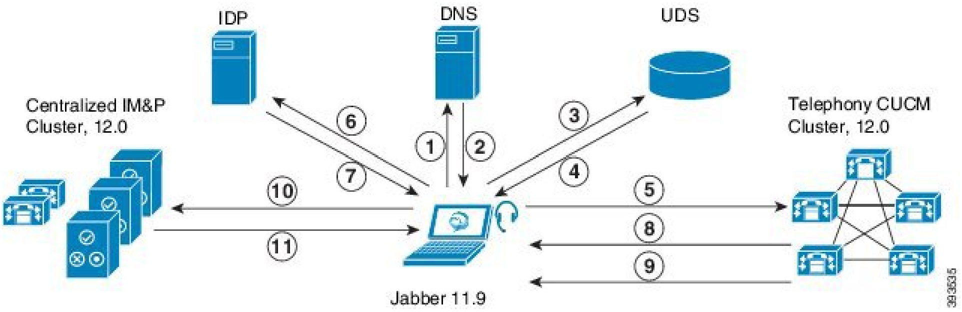
Advantages:
1. No full mesh, easy management for large deployment;
2. Version independent from Telephony CUCM cluster;
3. Lower cost option for customers with many clusters;
4. Easy XMPP federation with 3rd parties;

Centralized Cluster Use Case

To connect your telephony and IM and Presence clusters, a new system for exchanging access keys is introduced. This diagram shows the flow for SSO logins:

- [1]-[2]: Query DNS to get SRV record.
- [3]-[4]: Query UDS to get the Home Cisco Unified Communications Manager cluster.
- [5]-[8]: Get Access Token and Refresh Token from Cisco Unified Communications Manager cluster through SAML SSO.
- [9]: Read UC Service Profile. The service profile contains an IM and Presence profile and points to the IM and Presence central cluster.
- [10]: Client registers to the IM and Presence cluster using the same Access Token through SOAP and XMPP interfaces.
- [11]: The token is validated and a response is sent back to Jabber client.

Figure 2: IM and Presence Service Centralized Cluster Use Case



Centralized Deployment Prerequisites

The following requirements apply for the IM and Presence Service centralized deployment:

- The IM and Presence Service central cluster must be running Release 11.5(1)SU4 or higher.
- The local Cisco Unified Communications Manager instance that runs with the IM and Presence central cluster must be running the same release as the IM and Presence central cluster.
- The remote Cisco Unified Communications Manager telephony cluster must be running Release 10.5(2) or higher.
- Cisco Jabber must be running Release 11.9 or higher.
- For Push Notifications instant messaging support, the IM and Presence Service must be running at least 11.5(1)SU4.
- Cisco Unified Communications Manager functionality is based on the Cisco Unified Communications Manager version that is running on your remote telephony clusters rather than on the local instance that runs with the IM and Presence central cluster. For example:
    - For Push Notifications call support, the remote telephony cluster must be running at least 11.5(1)SU4.
    - For OAuth Refresh Logins support, the remote Cisco Unified Communications Manager telephony cluster must be running at least 11.5(1)SU4.
    - For SAML SSO support, the remote telephony cluster must be running at least 11.5(1)SU4.
- The **Cisco AXL Web Service** feature service must be running in all clusters. This service is enabled by default, but you can confirm that it is activated from the **Service Activation** window of Cisco Unified Serviceability.
- With Centralized Deployments, rich presence is handled by Cisco Jabber. The user's phone presence displays only if the user is logged in to Cisco Jabber.

DNS Requirements

The IM and Presence central cluster must have a DNS SRV record that points to the publisher node of the Cisco Unified Communications Manager telephony cluster. If your telephony deployment includes an ILS network, the DNS SRV must point to the hub cluster. This DNS SRV record should be referring to "_cisco-uds".

The SRV record is a Domain Name System (DNS) resource record that is used to identify computers that host specific services. SRV resource records are used to locate domain controllers for Active Directory. To verify SRV locator resource records for a domain controller, use the following method:

Active Directory creates its SRV records in the following folders, where Domain Name indicates the name of the installed domain:

- Forward Lookup Zones/Domain_Name/_msdcs/dc/_sites/Default-First-Site-Name/_tcp
- Forward Lookup Zones/Domain_Name/_msdcs/dc/_tcp

In these locations, an SRV record should appear for the following services:

- _kerberos
- _ldap
- _cisco_uds : indicates the SRV record

The below mentioned parameters has to be set during the SRV record creation .

- Service :_cisco_uds
- Protocol : _tcp
- weight : starts from 0 (0 is the highest priority)
- port no : 8443
- host : fqdn name of the server

An example of a DNS SRV record from a computer running a Jabber client is:

```
nslookup -type=all _cisco-uds._tcp.dcloud.example.com
Server: ad1.dcloud.example.com
Address: x.x.x.x
_cisco-uds._tcp.dcloud.example.com SRV service location:
priority = 10
weight = 10
port = 8443
svr hostname = cucm2.dcloud.example.com
cucm2.dcloud.example.com internet address = x.x.x.y
```

Centralized Deployment Configuration Task Flow

Complete these tasks if you want to configure a new IM and Presence Service deployment to use the centralized deployment option.

Note Use this task flow for new IM and Presence Service deployments only. If all of your users are migrating from existing decentralized IM and Presence clusters, refer to Migrate Users to Centralized Deployment , on page 77.

Table 14: Centralized Cluster Configuration Task Flow

	IM and Presence Central Cluster	Remote Telephony Clusters	Purpose
Step 1	Enable IM and Presence via Feature Group Template, on page 64		In your IM and Presence central cluster, configure a template that enables the IM and Presence Service.
Step 2	Complete LDAP Sync on IM and Presence Central Cluster, on page 64		Complete an LDAP sync to propagate settings to LDAP-synced users in your IM and Presence central cluster.
Step 3	Enable Users for IM and Presence via Bulk Admin, on page 65		Optional. If you have already completed an LDAP sync, use Bulk Administration to enable IM and Presence for users.
Step 4	Add Remote Telephony Clusters, on page 66		Add your remote telephony clusters to the IM and Presence central cluster.
Step 5		Configure an IM and Presence UC Service, on page 67	In your telephony clusters, add a UC service that points to the IM and Presence central cluster.
Step 6		Create Service Profile for IM and Presence, on page 68	Add your IM and Presence UC service to a service profile. Cisco Jabber clients ustep e this profile to find the IM and Presence central cluster.
Step 7		Disable Presence Users in Telephony Cluster, on page 68	In the telephony cluster, edit Presence user settings to point to the IM and Presence central cluster.
Step 8		Configure OAuth Refresh Logins , on page 69	Configuring OAuth in the telephony cluster will enable the feature for the central cluster.
Step 9		Configure an ILS Network, on page 70	If more than one telephony cluster exists,you must configure ILS.
Step 10		MRA Configuration	Configuration of MRA in case of centralized deployment.

What to do Next

If you want to connect your central cluster to other IM and Presence clusters as part of an intercluster network, configure intercluster peering.

Enable IM and Presence via Feature Group Template

Use this procedure to configure a feature group template with IM and Presence settings for the central cluster. You can add the feature group template to an LDAP Directory configuration to configure IM and Presence for synced users.

Note You can apply a feature group template only to an LDAP directory configuration where the initial sync has not yet occurred. Once you've synced your LDAP configuration from the central cluster, you cannot apply edits to the LDAP configuration in Cisco Unified Communications Manager. If you have already synced your directory, you will need to use Bulk Administration to configure IM and Presence for users. For details, see Enable Users for IM and Presence via Bulk Admin, on page 65.

Procedure

Step 1 Log into the Cisco Unified CM Administration interface of the IM and Presence centralized cluster. This server should have no telephony configured.

Step 2 Choose **User Management** > **User Phone/Add** > **Feature Group Template**.

Step 3 Do one of the following:

- Click **Find** and select an existing template
- Click **Add New** to create a new template

Step 4 Check both of the following check boxes:

- **Home Cluster**
- **Enable User for Unified CM IM and Presence**

Step 5 Complete the remaining fields in the **Feature Group Template Configuration** window. For help with the fields and their settings, refer to the online help.

Step 6 Click **Save**.

What to do next

To propagate the setting to users, you must add the Feature Group Template to an LDAP directory configuration where the initial sync has not yet occurred, and then complete the initial sync.

Complete LDAP Sync on IM and Presence Central Cluster, on page 64

Complete LDAP Sync on IM and Presence Central Cluster

Complete an LDAP sync on your IM and Presence Service central cluster to configure users with IM and Presence services via the feature group template.

Note You cannot apply edits to an LDAP sync configuration after the initial sync has occured. If the initial sync has already occurred, use Bulk Administration instead. For additional detail on how to set up an LDAP Directory sync, see the "Configure End Users" part of the *System Configuration Guide for Cisco Unified Communications Manager*.

Before you begin

Enable IM and Presence via Feature Group Template, on page 64

Procedure

Step 1 Log into the Cisco Unified CM Administration interface of the IM and Presence centralized cluster. This server should have no telephony configured.

Step 2 Choose **System** > **LDAP** > **LDAP Directory**.

Step 3 Do either of the following:

a) Click **Find** and select an existing LDAP Directory sync.

b) Click **Add New** to create a new LDAP Directory.

Step 4 From the **Feature Group Template** drop-down list box, select the IM and Presence-enabled feature group template that you created in the previous task.

Step 5 Complete the remaining fields in the **LDAP Directory** window. For help with the fields and their settings, refer to the online help.

Step 6 Click **Save**.

Step 7 Click **Perform Full Sync**.

Cisco Unified Communications Manager synchronizes the database with the external LDAP directory. End users are configured with IM and Presence services.

What to do next

Add Remote Telephony Clusters, on page 66

Enable Users for IM and Presence via Bulk Admin

If you have already synced users into the central cluster, and those users were not enabled for the IM and Presence Service, use Bulk Administration's Update Users feature to enable those users for the IM and Presence Service.

Note You can also use Bulk Administration's Import Users or Insert Users feature to import new users via a csv file. For procedures, see the *Bulk Administration Guide for Cisco Unified Communications Manager*. Make sure that imported users have the below options selected.

- Home Cluster
- Enable User for Unified CM IM and Presence

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **Users** > **Update Users** > **Query**.

Step 2 From the **Filter**, select **Has Home Cluster Enabled** and click **Find**. The window displays all of the end users for whom this is their Home Cluster

Step 3 Click **Next**.
In the **Update Users Configuration** window, the check boxes on the far left indicate whether you want to edit this setting with this query. If you don't check the left check box, the query will not update that field. The field on the right indicates the new setting for this field. If two check boxes appear, you must check the check box on the left to update the field, and in the right check box, enter the new setting.

Step 4 Under **Service Settings**, check the left check box for each of the following fields to indicate that you want to update these fields, and then edit the adjacent field setting as follows:

- **Home Cluster**—Check the right check box to enable this cluster as the home cluster.
- **Enable User for Unified CM IM and Presence**—Check the right check box. This setting enables the central cluster as the provider of IM and Presence Service for these users.

Step 5 Complete any remaining fields that you want to update. For help with the fields and their settings, see the online help:

Step 6 Under **Job Information**, select **Run Immediately**.

Step 7 Click **Submit**.

Add Remote Telephony Clusters

Use this procedure to add your remote telephony clusters to the centralized IM and Presence Service cluster.

Note If you have more than one telephony cluster, you must deploy ILS. In this case, the telephony cluster to which the IM and Presence central cluster connects must be a hub cluster.

Procedure

Step 1 Log in to database publisher node on the IM and Presence Service centralized cluster.

Step 2 From Cisco Unified CM IM and Presence Administration, choose **System** > **Centralized Deployment**.

Step 3 Click **Find** to view the list of current remote Cisco Unified Communications Manager clusters. If you want to edit the details of a cluster, select the cluster and click **Edit Selected**.

Step 4 Click **Add New** to add a new remote Cisco Unified Communications Manager telephony cluster.

Step 5 Complete the following fields for each telephony cluster that you want to add:

- **Peer Address**—The FQDN, hostname, IPv4 address, or IPv6 address of the publisher node on the remote Cisco Unified Communications Manager telephony cluster.
- **AXL Username**—The login username for the AXL account on the remote cluster.
- **AXL Password**—The password for the AXL account on the remote cluster.

Step 6 Click the **Save and Synchronize** button.
The IM and Presence Service synchronizes keys with the remote cluster.

What to do next

Configure an IM and Presence UC Service, on page 67

Configure an IM and Presence UC Service

Use this procedure in your remote telephony clusters to configure a UC service that points to the IM and Presence Service central cluster. Users in the telephony cluster will get IM and Presence services from the IM and Presence central cluster.

Procedure

Step 1 Log in to the Cisco Unified CM Administration interface on your telephony cluster.

Step 2 Choose **User Management** > **User Settings** > **UC Service**.

Step 3 Do either of the following:

a) Click **Find** and select an existing service to edit.

b) Click **Add New** to create a new UC service.

Step 4 From the **UC Service Type** drop-down list box, select **IM and Presence** and click **Next**.

Step 5 From the **Product type** drop-down list box, select **IM and Presence Service**.

Step 6 Enter a unique **Name** for the cluster. This does not have to be a hostname.

Step 7 From **HostName/IP Address**, enter the hostname, IPv4 address, or IPv6 address of the IM and Presence central cluster database publisher node.

Step 8 Click **Save**.

Step 9 Recommended. Repeat this procedure to create a second IM and Presence service where the **HostName/IP Address** field points to a subscriber node in the central cluster.

What to do next

Create Service Profile for IM and Presence, on page 68.

Create Service Profile for IM and Presence

Use this procedure in your remote telephony clusters to create a service profile that points to the IM and Presence central cluster. Users in the telephony cluster will use this service profile to get IM and Presence services from the central cluster.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Service Profile**.

Step 2 Do one of the following:

a) Click **Find** and select an existing service profile to edit.
b) Click **Add New** to create a new service profile.

Step 3 In the **IM and Presence Profile** section, configure IM and Presence services that you configured in the previous task:

a) From the **Primary** drop-down, select the database publisher node service.
b) From the **Secondary** drop-down, select the subscriber node service.

Step 4 Click **Save**.

What to do next

Disable Presence Users in Telephony Cluster, on page 68

Disable Presence Users in Telephony Cluster

If you've already completed an LDAP sync in your telephony deployment, use the Bulk Administration Tool to edit user settings in the Telephony cluster for IM and Presence users. This configuration will point Presence users to the Central Cluster for the IM and Presence Service.

Note This procedure assumes that you have already completed an LDAP sync in your telephony cluster. However, if you haven't yet completed the initial LDAP sync, you can add the Central Deployment settings for Presence users into your initial sync. In this case, do the following in your telephony cluster:

- Configure a Feature Group Template that includes the **Service Profile** that you just set up. Make sure that have the **Home Cluster** option selected and the **Enable User for Unified CM IM and Presence** option unselected.
- In **LDAP Directory Configuration**, add the **Feature Group Template** to your LDAP Directory sync.
- Complete the initial sync.

For additional details on configuring Feature Group Templates and LDAP Directory, see the "Configure End Users" part of the *System Configuration Guide for Cisco Unified Communications Manager*.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Query** > **Bulk Administration** > **Users** > **Update Users** > **Query**.

Step 2 From the Filter, select **Has Home Cluster Enabled** and click **Find**. The window displays all of the end users for whom this is their Home Cluster.

Step 3 Click **Next**.
In the **Update Users Configuration** window, the check boxes on the far left indicate whether you want to edit this setting with this query. If you don't check the left check box, the query will not update that field. The field on the right indicates the new setting for this field. If two check boxes appear, you must check the check box on the left to update the field, and in the right check box, enter the new setting.

Step 4 Under **Service Settings**, check the far left check box for each of the following fields to indicate that you want to update these fields, and then edit the adjacent setting as follows:

- **Home Cluster**—Check the right check box to enable the telephony cluster as the home cluster.
- **Enable User for Unified CM IM and Presence**—Leave the right check box unchecked. This setting disables the telephony cluster as the provider of IM and Presence.
- **UC Service Profile**—From the drop-down, select the service profile that you configured in the previous task. This setting points users to the IM and Presence central cluster, which will be the provider of the IM and Presence Service.

Note For Expressway MRA configuration, see *Mobile and Remote Access via Cisco Expressway Deployment Guide* at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.

Step 5 Complete any remaining fields that you want. For help with the fields and their settings, see the online help.

Step 6 Under **Job Information**, select **Run Immediately**.

Step 7 Click **Submit**.

What to do next

Configure OAuth Refresh Logins , on page 69

Configure OAuth Refresh Logins

Enable OAuth Refresh Logins in the telephony cluster. This will enable the feature in the central clsuter as well.

Procedure

Step 1 Log in to Cisco Unified CM Administration on the telephony cluster.

Step 2 Choose **System** > **Enterprise Parameters**.

Step 3 Under **SSO And OAuth Configuration,** set the **OAuth with Refresh Login Flow** enterprise parameter to **Enabled**.

Step 4 If you edited the parameter setting, click **Save**.

Configure an ILS Network

For IM and Presence centralized clusters where there are more than one remote telephony clusters, you can use the Intercluster Lookup Service (ILS) to provision remote telephony clusters for the IM and Presence central cluster. ILS monitors the network and propagates network changes such as new clusters or address changes to the entire network.

Note This task flow focuses on ILS requirements around IM and Presence centralized cluster deployments. For additional ILS configuration around telephony, such as configuring Global Dial Plan Replication or URI Dialing, see the "Configure the Dial Plan" section of the *System Configuration Guide for Cisco Unified Communications Manager*.

Before you begin

If you are deploying ILS, make sure that you have done the following:

- Plan your ILS network topology. You must know which telephony clusters will be hubs and spokes.
- The telephony cluster to which the IM and Presence central cluster connects must be a hub cluster.
- You must configure a DNS SRV record that points to the publisher node of the hub cluster.

For information on designing an ILS network, see the *Cisco Collaboration System Solution Reference Network Design* at http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html.

Procedure

	Command or Action	Purpose
Step 1	Configure Cluster IDs for ILS, on page 71	Set unique Cluster IDs for each telephony cluster. ILS will not work while the Cluster ID is set to `StandAloneCluster` (the default setting).
Step 2	Enable ILS on Telephony Clusters, on page 71	Configure and activate ILS on the publisher node of each telephony cluster in the ILS network.
Step 3	Verify ILS Network is Running, on page 72	When ILS is working, you can see all of your remote clusters from the **ILS Configuration** window of your telephony clusters with an "Up to Date" synchronization status.

Configure Cluster IDs for ILS

Each cluster within the ILS network must have a unique Cluster ID. Use this procedure to give your telephony clusters unique cluster IDs.

Procedure

Step 1 Log in to Cisco Unified CM Administration on the publisher node.

Step 2 Choose **System** > **Enterprise Parameters**.

Step 3 Change the value of the **Cluster ID** parameter from `StandAloneCluster` to a unique value that you set. ILS will not work while the Cluster ID is `StandAloneCluster`.

Step 4 Click **Save**.

Step 5 Repeat this procedure on the publisher node of each telephony cluster that you want to join into the ILS network. Each cluster must have a unique ID.

What to do next

Enable ILS on Telephony Clusters, on page 71

Enable ILS on Telephony Clusters

Use this procedure to configure and activate ILS on your Cisco Unified Communications Manager telephony clusters.

Note

- Configure your hub clusters before configuring your spoke clusters.
- For help with the fields and their settings, refer to the online help.

Before you begin

Configure Cluster IDs for ILS, on page 71

Procedure

Step 1 Log into Cisco Unified CM Administration on the publisher node of your telephony cluster.

Step 2 Choose **Advanced Features** > **ILS Configuration**.

Step 3 From the **Role** drop-down list box, select **Hub Cluster** or **Spoke Cluster** depending on which type of cluster you are setting up.

Step 4 Check the **Exchange Global Dial Plan Replication Data with Remote Clusters** check box.

Step 5 Configure **ILS Authentication Details**.

a) If you want to use TLS authentication between the various clusters, check the **Use TLS Certificates** check box.

Note If you use TLS, you must exchange CA-signed certificates between the nodes in your cluster.

b) If you want to use password authentication (regardless of whether TLS is used), check the **Use Password** check box and enter the password details.

Step 6 Click **Save**.

Step 7 In the **ILS Cluster Registration** popup, configure your registration details:

- In the **Registration Server** text box, enter the publisher node IP address or FQDN for the hub cluster to which you want to connect this cluster. If this is the first hub cluster in your network, you can leave the field blank.
- Make sure that the **Activate the Intercluster Lookup Service on the publisher in this cluster** check box is checked.

Step 8 Click **OK**.

Step 9 Repeat this procedure on the publisher node of each telephony cluster that you want to add to the ILS network. Depending on the sync values that you configured, there may be a delay while the cluster information propagates throughout the network.

If you chose to use Transport Layer Security (TLS) authentication between clusters, you must exchange Tomcat certificates between the publisher node of each cluster in the ILS network. From Cisco Unified Operating System Administration, use the Bulk Certificate Management feature to:

- Export certificates from the publisher node of each cluster to a central location
- Consolidate exported certificates in the ILS network
- Import certificates onto the publisher node of each cluster in your network

For details, see the "Manage Certificates" chapter of the *Administration Guide for Cisco Unified Communications Manager*.

What to do next

After ILS is up and running, and you have exchanged certificates (if required), Verify ILS Network is Running, on page 72

Verify ILS Network is Running

Use this procedure to confirm that your ILS network is up and running.

Procedure

Step 1 Log in to the publisher node on any of your telephony clusters.

Step 2 From Cisco Unified CM Administration choose **Advanced Features** > **ILS Configuration**.

Step 3 Check the **ILS Clusters and Global Dial Plan Imported Catalogs** section. Your ILS network topology should appear.

MRA Configuration

Cisco Unified Communications Mobile and Remote Access is a core part of the Cisco Collaboration Edge Architecture. It allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging and presence services provided by Cisco Unified Communications Manager when the endpoint is not within the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations.

The overall solution provides :

1. **Off-premises access** : A consistent experience outside the network for Jabber and EX/MX/SX series clients.
2. **Security** : Secure business-to-business communications.
3. **Cloud services** : Enterprise grade flexibility and scalable solutions providing rich WebEx integration and Service Provider offerings.
4. **Gateway and interoperability services** : Media and signalling normalization, and support for non-standard endpoints.

Configuration

To configure MRA on all telephony leaf clusters in Expressway-C. Choose **Configuration → Unified Communications → Unified CM Servers**.

To configure MRA on centralized IM&P nodes cluster in Expressway-C. Choose **Configuration→ Unified Communications → IM and Presence Service nodes**.

To Enable the **"Mobile and Remote Access"**in Expressway-C. Choose **Configuration → Enable "Mobile and Remote Access"** and select the control options as per the table below.

Table 15: OAuth Enable Configuration

Authentication path	UCM / LADP basic authentication
Authorize by OAuth token with refresh	ON
Authorize by OAuth token	ON
Authorize by user credentia	No
Allow Jabber iOS clients to use embedded Safari browser	No
Check for internal authentication availability	Yes

Table 16: OAuth Disable Configuration

Authentication path	UCM / LADP basic authentication
Authorize by OAuth token with refresh	Off
Authorize by user credentia	On
Allow Jabber iOS clients to use embedded Safari browser	Off
Check for internal authentication availability	Yes

Note **For Information on Basic MRA Configuration , Please refer :** https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

Centralized Deployment Field Descriptions

From Cisco Unified CM IM and Presence Administration, choose **System** > **Centralized Deployment** to access the Centralized Deployment window. If you are deploying the IM and Presence Centralized Cluster deployment, you can create connections to your remote Cisco Unified Communications Manager clusters in this configuration window.

Click the **Add New** button to add a Cisco Unified Communications Manager cluster. Click **Synchronize Selected** to synchronize access keys with the remote cluster.

Table 17: Centralized Deployment Field Descriptions

Field	Description
Peer Address	The FQDN, hostname, IPv4 address, or IPv6 address of the remote Cisco Unified Communications Manager cluster publisher node. **Note** The Peer Address cannot point to any IM and Presence Service node or to the Cisco Unified Communications Manager instance of another IM and Presence Service central cluster.
Peer AXL Username	The login username for the AXL account on the remote cluster.
Peer AXL Password	The password for the AXL account on the remote cluster.
Status	Displays the current sync status with the remote cluster.
Last Synchronized	Displays the last time a sync occurred with the remote cluster.
Save and Synchronize	After you have entered your details, click this button to save your settings and to sync access keys with the remote cluster.

Centralized Deployment Interactions and Restrictions

Feature	Interaction
ILS Hub Cluster	If the ILS hub cluster is down, and more than one telephony cluster exists, the Central Cluster feature does not work.
ILS Deployments	If you are deplying an IM and Presence central cluster and you are also deploying ILS, you can deploy ILS in the telephony clusters only. You cannot deploy ILS on the Cisco Unified Communications Manager instance for the IM and Presence central cluster. This instance is for provisioning only and does not handle telephony.

Feature	Interaction
Rich Presence	In a Centralized deployment, users' rich presence is computed by Cisco Jabber. Users' telephony presence is displayed only when if the user is logged in to Jabber.
Unified Communications Manager Cluster Status	In a centralized deployment, the Unified Communications Manager cluster status appears as**Synchronized for OAuth Refresh Logins**. This feature is available from 11.5(1)SU3 onwards. When you add a Unified Communications Manager cluster to 11.5(1)SU3 or earlier release, the cluster status appears as Unsynchronized under Cisco Unified CM IM and Presence Administration, **System** > **Centralized Deployment** as it does not support OAuth Refresh Logins. Whereas these clusters are compatible for centralized IM and Presence Service deployment using SSO or LDAP directory credentials. **Note** There is no functional impact on Cisco Jabber user login.

CHAPTER 7

Migrate Users to Centralized Deployment

- Centralized Deployment User Migration Overview, on page 77
- Prerequisite Tasks for Central Cluster Migration, on page 77
- Migration to Central Cluster Task Flow, on page 78

Centralized Deployment User Migration Overview

This chapter contains procedures for migrating existing IM and Presence Service users from a standard decentralized IM and Presence deployment (IM and Presence Service on Cisco Unified Communications Manager) to a centralized deployment. With the centralized deployment, the IM and Presence deployment and the telephony deployment are in separate clusters.

Prerequisite Tasks for Central Cluster Migration

If you are setting up a new IM and Presence central cluster whereby all the users are migrating from existing decentralized clusters, complete the following prerequisite steps to set up the cluster for migration.

Note If you are adding new users whom are not a part of the migration, you can follow the instructions in Configure Centralized Deployment, on page 57 to set up the central cluster with your new users. Migrate existing users to the central cluster only after you are confident that your configuration works.

Table 18: Pre-Migration Tasks

	Pre-Migration Tasks
Step 1	Connect your new central cluster to the migrating cluster. 1. Log in to database publisher node on the IM and Presence Service centralized cluster. 2. From Cisco Unified CM IM and Presence Administration, choose **System** > **Centralized Deployment**. 3. Click **Find** and do either of the following: • Select an existing cluster and click **Edit Selected**. • Click **Add New** to add the migrating cluster. 4. Complete the following fields for each migrating cluster: • **Peer Address**—The FQDN, hostname, IPv4 address, or IPv6 address of the publisher node on the remote telephony • **AXL Username**—The login username for the AXL account on the remote telephony cluster. • **AXL Password**—The password for the AXL account on the remote cluster. 5. Click **Save**.
Step 2	If the new central cluster will be part of an IM and Presence intercluster network, configure intercluster peering between the central cluster and any IM and Presence peer clusters that are not a part of the migration. The following guidelines apply: • You do not need to configure intercluster peering between the central cluster and the migrating clusters. However, if a migrating cluster has an intercluster peer connection configured with any number of non-migrating clusters at the time of the migration, it's mandatory that those intercluster peer connections are configured in the central cluster prior to the migration or the migration will not work. • After configuring intercluster peering, make sure to verify the intercluster peering status to ensure that the configuration works properly For details, see the Intercluster Peering configuration topics in the *Configuration and Administration Guide for the IM and Presence Service.*

Migration to Central Cluster Task Flow

Complete these tasks to migrate existing users from a decentralized cluster (IM and Presence Service on Cisco Unified Communications Manager) to a centralized IM and Presence cluster. In this task flow:

- **IM and Presence Central Cluster** refers to the cluster to which you are migating users. Following the migration, this cluster handles IM and Presence only.

- **Migrating Cluster** refers to the cluster from which IM and Presence users are being migrated. Following the migration, this cluster handles telephony only.

Before You Begin

If your IM and Presence central cluster is a newly installed cluster, and does not yet have users, complete the Prerequisite Tasks for Central Cluster Migration, on page 77 before you migrate users.

Table 19: Migration to Central Cluster Task Flow

	IM and Presence Central Cluster	Migrating Cluster	Purpose
Step 1		Export Contact Lists from Migrating Cluster, on page 80	Export user contact lists in the migrating cluster to a csv file.
Step 2		Disable High Availability in Migrating Cluster, on page 81	Disable High Availability for all Presence Redundancy Groups (subclusters) in the migrating cluster.
Step 3		Configure UC Service for IM and Presence, on page 82	In the migrating cluster, configure IM and Presence UC services that point to the IM and Presence central cluster.
Step 4		Create Service Profile for IM and Presence, on page 82	In the migrating cluster, create a service profile that uses the IM and Presence UC services that you set up.
Step 5		Disable Presence Users in Telephony Cluster, on page 83	Use Bulk Administration in the migrating cluster to disable IM and Presence for users.
Step 6		Enable OAuth Authentication for Central Cluster, on page 84	Optional. In the migrating cluster, enable OAuth Refresh Logins. This will enable the feature for the central cluster as well.
Step 7	Disable High Availability in Central Cluster, on page 84		Disable High Availability in all Presence Redundancy Groups (subcluster) of the IM and Presence central cluster.
Step 8	Delete Peer Relationship for Central and Migrating Clusters, on page 85		If intercluster peering exists between the central cluster and migrating cluster, delete the peer connection on both clusters.

	IM and Presence Central Cluster	Migrating Cluster	Purpose
Step 9	Stop the Cisco Intercluster Sync Agent, on page 85		Stop the Cisco Intercluster Sync Agent in the IM and Presence central cluster.
Step 10	Enable IM and Presence via Feature Group Template, on page 86		In the cenral cluster, configure a Feature Group Template that enables the IM and Presence Service.
Step 11	Complete LDAP Sync on Central Cluster, on page 86		Add the feature group template to an LDAP directory sync. Use the sync to add users from the migrating cluster.
Step 12	Import Contact Lists into Central Cluster, on page 88		Use Bulk Administration and the csv export file that you created earlier to import contact lists into the central cluster.
Step 13	Start Cisco Intercluster Sync Agent, on page 89		Start the Cisco Intercluster Sync Agent in the central cluster.
Step 14	Enable High Availability in Central Cluster, on page 89		In the central cluster, enable High Availability in all Presence Redundancy Groups.
Step 15		Delete Remaining Peers for Migrating Cluster, on page 90	Delete remaining intercluster peer connections between migrating cluster (now a telephony cluster) and other peer clusters.

Export Contact Lists from Migrating Cluster

Use this procedure only if you are migrating from a Decentralized IM and Presence Deployment to a Centralized Deployment. In the migrating cluster, export your users' contact lists to a csv file that you will later be able to import into the central cluster. You can export two types of contact lists:

- Contact Lists—This list consists of IM and Presence contacts. Contacts whom do not have an IM address will not be exported with this list (you must export a non-presence contact list).
- Non-presence Contact Lists—This list consists of contacts whom do not have an IM address.

Procedure

Step 1 Log in to Cisco Unified CM IM and Presence Administration in the old clsuter (the telephony cluster).

Step 2 Choose one of the following options, depending on which type of contact list you want to export:

- For Contact List exports, choose **Bulk Administration** > **Contact List** > **Export Contact List**
- for Non-presence Contact List exports, choose **Bulk Administration** > **Non-presence Contact List** > **Export Non-presence Contact List** and skip the next step.

Step 3 Contact Lists only. Select the users for whom you will export contact lists:

a) Under **Export Contact List Options**, choose the category of users for whom you will export contact lists. The default option is **All users in the cluster**.

b) Click **Find** to bring up the list of users and then click **Next**.

Step 4 Enter a **File Name**.

Step 5 Under **Job Information**, configure when you want to run this job:

- **Run Immediately**—Check this button to export contact lists right away.
- **Run Later**—Check this button if you want to schedule a time for the job to run.

Step 6 Click **Submit**.

Note If you chose **Run Immediately**, your export file gets generated right away. If you chose **Run Later**, you must use the Job Scheduler at (**Bulk Administration** > **Job Scheduler**) to schedule a time for this job to run.

Step 7 After the export file is generated, download the csv file:

a) Choose **Bulk Administration** > **Upload/Download Files**.

b) Click **Find**.

c) Select the export file that you want to download and click **Download Selected**.

d) Save the file to a safe location.

Step 8 Repeat this procedure if you want to create another csv export file. For example, if you create an export file for Contact Lists, you may want to create another file for Non-presence Contact Lists.

What to do next

Disable High Availability in Migrating Cluster, on page 81

Disable High Availability in Migrating Cluster

For migrations to a Centralized Deployment, disable High Availability in each Presence Redundancy Group (subcluster) on the migrating telephony cluster.

Procedure

Step 1 Log in to the Cisco Unified Communications Manager publisher node on the old cluster.

Step 2 From Cisco Unified CM Administration, choose **System** > **Presence Redundancy Groups**.

Step 3 Click **Find** and select a subcluster.

Step 4 Uncheck the **Enable High Availability** check box.

Step 5 Click **Save**.

Step 6 Repeat this procedure for each subcluster.

Note After completing this procedure for all subclusters, wait at least 2 minutes before completing any additional configurations on this cluster.

What to do next

Configure UC Service for IM and Presence, on page 82

Configure UC Service for IM and Presence

Use this procedure in your remote telephony clusters to configure a UC service that points to the IM and Presence Service central cluster. Users in the telephony cluster will get IM and Presence services from the IM and Presence central cluster.

Procedure

Step 1 Log in to the Cisco Unified CM Administration interface on your telephony cluster.

Step 2 Choose **User Management** > **User Settings** > **UC Service**.

Step 3 Do either of the following:

a) Click **Find** and select an existing service to edit.

b) Click **Add New** to create a new UC service.

Step 4 From the **UC Service Type** drop-down list box, select **IM and Presence** and click **Next**.

Step 5 From the **Product type** drop-down list box, select **IM and Presence Service**.

Step 6 Enter a unique **Name** for the cluster. This does not have to be a hostname.

Step 7 From **HostName/IP Address**, enter the hostname, IPv4 address, or IPv6 address of the IM and Presence central cluster database publisher node.

Step 8 Click **Save**.

Step 9 Recommended. Repeat this procedure to create a second IM and Presence service where the **HostName/IP Address** field points to a subscriber node in the central cluster.

What to do next

Create Service Profile for IM and Presence, on page 82

Create Service Profile for IM and Presence

Use this procedure in your remote telephony clusters to create a service profile that points to the IM and Presence central cluster. Users in the telephony cluster will use this service profile to get IM and Presence services from the central cluster.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Service Profile**.

Step 2 Do one of the following:

a) Click **Find** and select an existing service profile to edit.

b) Click **Add New** to create a new service profile.

Step 3 In the **IM and Presence Profile** section, configure IM and Presence services that you configured in the previous task:

a) From the **Primary** drop-down, select the database publisher node service.

b) From the **Secondary** drop-down, select the subscriber node service.

Step 4 Click **Save**.

What to do next

Disable Presence Users in Telephony Cluster, on page 83

Disable Presence Users in Telephony Cluster

If you've already completed an LDAP sync in your telephony deployment, use the Bulk Administration Tool to edit user settings in the Telephony cluster for IM and Presence users. This configuration will point Presence users to the Central Cluster for the IM and Presence Service.

Note This procedure assumes that you have already completed an LDAP sync in your telephony cluster. However, if you haven't yet completed the initial LDAP sync, you can add the Central Deployment settings for Presence users into your initial sync. In this case, do the following in your telephony cluster:

- Configure a Feature Group Template that includes the **Service Profile** that you just set up. Make sure that have the **Home Cluster** option selected and the **Enable User for Unified CM IM and Presence** option unselected.
- In **LDAP Directory Configuration**, add the **Feature Group Template** to your LDAP Directory sync.
- Complete the initial sync.

For additional details on configuring Feature Group Templates and LDAP Directory, see the "Configure End Users" part of the *System Configuration Guide for Cisco Unified Communications Manager*.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Query** > **Bulk Administration** > **Users** > **Update Users** > **Query**.

Step 2 From the Filter, select **Has Home Cluster Enabled** and click **Find**. The window displays all of the end users for whom this is their Home Cluster.

Step 3 Click **Next**.
In the **Update Users Configuration** window, the check boxes on the far left indicate whether you want to edit this setting with this query. If you don't check the left check box, the query will not update that field. The field on the right indicates the new setting for this field. If two check boxes appear, you must check the check box on the left to update the field, and in the right check box, enter the new setting.

Step 4 Under **Service Settings**, check the far left check box for each of the following fields to indicate that you want to update these fields, and then edit the adjacent setting as follows:

- **Home Cluster**—Check the right check box to enable the telephony cluster as the home cluster.
- **Enable User for Unified CM IM and Presence**—Leave the right check box unchecked. This setting disables the telephony cluster as the provider of IM and Presence.
- **UC Service Profile**—From the drop-down, select the service profile that you configured in the previous task. This setting points users to the IM and Presence central cluster, which will be the provider of the IM and Presence Service.

Note For Expressway MRA configuration, see *Mobile and Remote Access via Cisco Expressway Deployment Guide* at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.

Step 5 Complete any remaining fields that you want. For help with the fields and their settings, see the online help.

Step 6 Under **Job Information**, select **Run Immediately**.

Step 7 Click **Submit**.

What to do next

Enable OAuth Authentication for Central Cluster, on page 84

Enable OAuth Authentication for Central Cluster

Use this procedure to enable OAuth authentication in the telephony cluster. This also enables OAuth authentication in the IM and Presence central cluster.

Procedure

Step 1 Log in to Cisco Unified CM Administration on the telephony cluster.

Step 2 Choose **System** > **Enterprise Parameters**

Step 3 Under **SSO And OAuth Configuration**, set the **OAuth with Refresh Login Flow** enterprise parameter to **Enabled**.

Step 4 If you edited the parameter setting, click **Save**.

Disable High Availability in Central Cluster

Make sure that High Availability is disabled in each Presence Redundancy Group (subcluster) of the IM and Presence central cluster. You must do this before you begin applying configurations or migrating users.

Procedure

Step 1 Log in to Cisco Unified CM Administration instance for the central cluster.

Step 2 Choose **System** > **Presence Redundancy Groups**.

Step 3 Click **Find** and select an existing subcluster.

Step 4 Uncheck the **Enable High Availability** check box.

Step 5 Click **Save**.

Step 6 Repeat this step for each subcluster.

What to do next

Stop the Cisco Intercluster Sync Agent, on page 85

Delete Peer Relationship for Central and Migrating Clusters

If intercluster peering exists between the IM and Presence central cluster and the migrating cluster, delete that peer relationship.

Procedure

Step 1 Log in to the IM and Presence Service central cluster's database publisher node.

Step 2 From Cisco Unified CM IM and Presence Administration, choose **Presence** > **Inter-Clustering**.

Step 3 Click **Find** and select the migrating cluster.

Step 4 Click **Delete**.

Step 5 Restart the **Cisco XCP Router**:

a) Log in to Unified IM and Presence Serviceability and choose **Tools** > **Control Center - Network Services**.
b) From the **Server** list, choose the database publisher node and click **Go**.
c) Under **IM and Presence Services**, select **Cisco XCP Router** and click **Restart**.

Step 6 Repeat these steps on the migrating cluster.

Stop the Cisco Intercluster Sync Agent

Before you configure the IM and Presence central cluster, make sure that the **Cisco Intercluster Sync Agent** service is stopped on the central cluster.

Procedure

Step 1 From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.

Step 2 From the **Server** drop-down, select the central cluster database publisher node, and click **Go**.

Step 3 Confirm the status of the **Cisco Intercluster Sync Agent** service. If the service is running or activated, select the adjacent radio button and click **Stop**.

What to do next

Enable IM and Presence via Feature Group Template, on page 86

Enable IM and Presence via Feature Group Template

Use this procedure to configure a feature group template with IM and Presence settings for the central cluster. You can add the feature group template to an LDAP Directory configuration to configure IM and Presence for synced users.

Note You can apply a feature group template only to an LDAP directory configuration where the initial sync has not yet occurred. Once you've synced your LDAP configuration from the central cluster, you cannot apply edits to the LDAP configuration in Cisco Unified Communications Manager. If you have already synced your directory, you will need to use Bulk Administration to configure IM and Presence for users. For details, see Enable Users for IM and Presence via Bulk Admin, on page 65.

Procedure

Step 1 Log into the Cisco Unified CM Administration interface of the IM and Presence centralized cluster. This server should have no telephony configured.

Step 2 Choose **User Management** > **User Phone/Add** > **Feature Group Template**.

Step 3 Do one of the following:

- Click **Find** and select an existing template
- Click **Add New** to create a new template

Step 4 Check both of the following check boxes:

- **Home Cluster**
- **Enable User for Unified CM IM and Presence**

Step 5 Complete the remaining fields in the **Feature Group Template Configuration** window. For help with the fields and their settings, refer to the online help.

Step 6 Click **Save**.

What to do next

To propagate the setting to users, you must add the Feature Group Template to an LDAP directory configuration where the initial sync has not yet occurred, and then complete the initial sync.

Complete LDAP Sync on Central Cluster, on page 86

Complete LDAP Sync on Central Cluster

Use this procedure on your remote Cisco Unified Communications Manager telephony clusters to use an LDAP sync to deploy your centralized IM and Presence settings to your Cisco Unified Communications Manager deployment.

Note For more details on how to set up an LDAP Directory sync, see the "Configure End Users" part of the *System Configuration Guide for Cisco Unified Communications Manager*.

Procedure

Step 1 From Cisco Unified CM Administration, choose the **System** > **LDAP** > **LDAP Directory**.

Step 2 Do either of the following:

- Click **Find** and select an existing LDAP Directory sync.
- Click **Add New** to create a new LDAP Directory sync.

Step 3 From the **Feature Group Template** drop-down list box, select the feature group template that you created in the previous task. IM and Presence must be disabled on this template.

Step 4 Complete the remaining fields in the **LDAP Directory** window. For help with the fields and their settings, refer to the online help.

Step 5 Click **Save**.

Step 6 Click **Perform Full Sync**.
Cisco Unified Communications Manager synchronizes its database with the LDAP directory and assigns the updated IM and Presence settings.

What to do next

Import Contact Lists into Central Cluster, on page 88

Enable Users for IM and Presence via Bulk Admin

If you have already synced users into the central cluster, and those users were not enabled for the IM and Presence Service, use Bulk Administration's Update Users feature to enable those users for the IM and Presence Service.

Note You can also use Bulk Administration's Import Users or Insert Users feature to import new users via a csv file. For procedures, see the *Bulk Administration Guide for Cisco Unified Communications Manager*. Make sure that imported users have the below options selected.

- Home Cluster
- Enable User for Unified CM IM and Presence

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **Users** > **Update Users** > **Query**.

Step 2 From the **Filter**, select **Has Home Cluster Enabled** and click **Find**. The window displays all of the end users for whom this is their Home Cluster

Step 3 Click **Next**.
In the **Update Users Configuration** window, the check boxes on the far left indicate whether you want to edit this setting with this query. If you don't check the left check box, the query will not update that field. The field on the right indicates the new setting for this field. If two check boxes appear, you must check the check box on the left to update the field, and in the right check box, enter the new setting.

Step 4 Under **Service Settings**, check the left check box for each of the following fields to indicate that you want to update these fields, and then edit the adjacent field setting as follows:

- **Home Cluster**—Check the right check box to enable this cluster as the home cluster.
- **Enable User for Unified CM IM and Presence**—Check the right check box. This setting enables the central cluster as the provider of IM and Presence Service for these users.

Step 5 Complete any remaining fields that you want to update. For help with the fields and their settings, see the online help:

Step 6 Under **Job Information**, select **Run Immediately**.

Step 7 Click **Submit**.

Import Contact Lists into Central Cluster

If you have migrated users to the IM and Presence Central Cluster, you can use this procedure to import your users' contact lists into the IM and Presence central cluster. You can import either of the following types of contact lists:

- Contact lists—This list contains IM and Presence contacts.
- Non-presence contact lists—This list contains contacts whom do not have an IM address.

Before you begin

You require the contact list csv file(s) that you exported from the old cluster (the telephony cluster).

Procedure

Step 1 Log in to Cisco Unified CM IM and Presence Administration on the IM and Presence central cluster.

Step 2 Upload the csv file that you exported from the telephony cluster:

a) Choose **Bulk Administration** > **Upload/Download Files**.
b) Click **Add New**.
c) Click **Choose File** and select the csv file that you want to import.
d) From the **Select the Target** drop-down select either of the following: **Contact Lists** or **Non-presence Contact Lists** depending on which type of contact list you are importing.
e) From the **Select Transaction Type**, select the import job.
f) Click **Save**.

Step 3 Import the csv information into the central cluster:

a) From Cisco Unified CM IM and Presence Administration, do either of the following:

- For Contact List imports, choose **Bulk Administration** > **Contact Lists** > **Update Contact Lists**.
- For Non-presence Contact List imports, choose **Bulk Administration** > **Non-presence Contact Lists** > **Import Non-presence Contact Lists**.

b) From the **File Name** drop-down, select the csv file that you uploaded.
c) Under **Job Information**, select either **Run Immediately** or **Run Later** depending on when you want the job to run.
d) Click **Submit**. If you chose **Run Immediately**, the contact lists get imported right away

Note . If you chose **Run Later**, you must go to **Bulk Administration** > **Job Scheduler** where you can select the job and schedule a time for it to run.

Step 4 Repeat this procedure if you have a second csv file to import.

What to do next

Start Cisco Intercluster Sync Agent, on page 89

Start Cisco Intercluster Sync Agent

After your configuration or migration is complete, start the **Cisco Intercluster Sync Agent** in the IM and Presence central cluster. This service is required if you are using intercluster peering.

Procedure

Step 1 From Cisco Unified IM and Presence Serviceability, choose **Tools** > **Control Center - Network Services**.

Step 2 From the **Server** drop-down, select the IM and Presence database publisher node and click **Go**.

Step 3 Under **IM and Presence Services**, select the **Cisco Intercluster Sync Agent** and click **Start**.

What to do next

Enable High Availability in Central Cluster, on page 89

Enable High Availability in Central Cluster

After your configuration or user migration is complete, enable High Availability in the Presence Redundancy Groups (subclusters) for the IM and Presence central cluster.

Procedure

Step 1 Log in to the Cisco Unified CM Administration instance on the IM and Presence central cluster.

Step 2 Choose **System** > **Presence Redundancy Groups**.

Step 3 Click **Find** and select an existing subcluster.

Step 4 Check the **Enable High Availability** check box.

Step 5 Click **Save**.

Step 6 Repeat this procedure for each subcluster in the IM and Presence central cluster.

Delete Remaining Peers for Migrating Cluster

Delete intercluster peer relationships between the migrating cluster (now a telephony cluster) and any remaining IM and Presence Service peer clusters.

Note Removing intercluster connections can be postponed to a later date depending on the Cisco XCP Router restart availability across the entire mesh. As long as there are existing intercluster connections between telephony cluster and any number of peer clusters, currently running Cisco XCP Router services should be kept in **Running** state on the telephony cluster.

Procedure

Step 1 Log in to the migrating cluster's IM and Presence database publisher node.

Step 2 From Cisco Unified CM IM and Presence Administration, choose **Presence** > **Inter-Clustering**.

Step 3 Click **Find** and select the peer cluster.

Step 4 Click **Delete**.

Step 5 Restart the **Cisco XCP Router**:

a) Log in to Unified IM and Presence Serviceability and choose **Tools** > **Control Center - Network Services**.
b) From the **Server** list, choose the database publisher node and click **Go**.
c) Under **IM and Presence Services**, select **Cisco XCP Router** and click **Restart**.

Step 6 Repeat these steps on the IM and Presence Service peer cluster.

Note If the migrating cluster has intercluster peer connections to multiple clusters, you must repeat this procedure for each peer cluster that remains in the intercluster network. This means that, on the migrating cluster, there will be as many cycles of **Cisco XCP Router** restarts as there are peer cluster connections that are being broken.