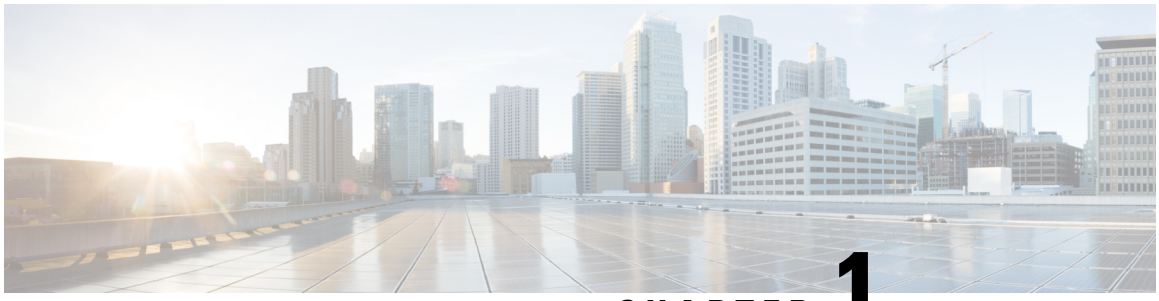
Release Notes for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5(1)SU3

First Published: 2017-08-17

Last Modified: 2020-12-13

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

Revision History

Date	Revision
June 07, 2019	Added link to Caveats in the Readme file.
August 17, 2017	Initial publish
October 06, 2017	Updated information related to documentation defect CSCvg10775.
October 12, 2017	Updated information related to release version.
November 2, 2017	Added important note on route filters and associated route patterns.
December 06, 2017	Added respin releases 11.5(1)SU3a and 11.5(1)SU3b to the Supported Versions list
December 22, 2017	Removed procedures for Office 365 calendar integration and redirected readers to the new *Microsoft Outlook Calendar Integration Guide* for configuration.
February 14, 2018	Added Important Note on persistent chat character limit when Microsoft SQL Server is the external database.
April 09, 2018	Added Documentation Update about the SIP Profile Settings information in the online help.
January 30, 2020	Added important note on gateway support

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 software versions are supported with Release 11.5(1)SU3:

- Cisco Unified Communications Manager 11.5.1.13902-2 (11.5(1)SU3b)
- Cisco Unified Communications Manager 11.5.1.13901-3 (11.5(1)SU3a)
- Cisco Unified Communications Manager 11.5.1.13900-52 (11.5(1)SU3)
- IM and Presence Service 11.5.1.13900-57

Version Mismatch Not Supported

For your 11.5(1)SU3 deployment to be supported, both Cisco Unified Communications Manager and IM and Presence Service must be running 11.5(1)SU3 versions. Running an 11.5(1)SU3 version of Cisco Unified Communications Manager with an earlier version of IM and Presence Service is not supported. Similarly, running an 11.5(1)SU3 version of IM and Presence Service with an earlier version of Cisco Unified Communications Manager is not supported.

Documentation for this Release

In addition to these Release Notes, the following documentation is published for this release:

New Documentation for this Release

The following table contains documents that were published specifically for the 11.5(1)SU3.

Table 1: Documentation for Release 11.5(1)SU3

Documents	Description
ReadMe Files for 11.5(1)SU3: • ReadMe File for Cisco Unified Communications Manager • ReadMe File for Cisco Unified CM IM and Presence Service	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.
Command Line Interface Reference Guide	Refer to this guide for the Command Line Interface (CLI) commands that are available for a Cisco Unified Communications Solution.
Database Setup Guide for the IM and Presence Service	Use this guide to configure an external database to store information synchronized from the IM and Presence Service. This release includes updates to the table values for Microsoft SQL Server external databases.
Deploying Push Notifications for Cisco Jabber for iPhone and iPad	This solution 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 Documentation from Release 11.5(x)

Where an 11.5(1)SU3 version of a document exists (for example, the *Database Setup Guide*), you should use the SU3 version. However, if no 11.5(1)SU3 version of that document exists, you can use existing 11.5(x) documentation. For information on the documentation set that is available for Release 11.5(x), refer to the *Documentation Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 11.5(1)* at:

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, SU6, SU7, SU8, and SU9 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, Unified Communications Manager cannot synchronize its license usage with the standalone Prime License Manager.

If you are upgrading to one of these 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 Unified Communications Manager.

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

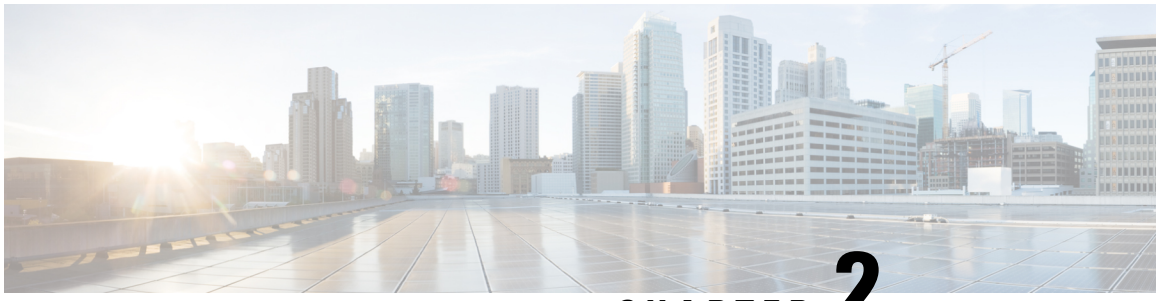
OpenJDK Migration

For this release, Cisco has migrated to the Open Java Development Kit (OpenJDK) platform from Oracle JDK for Cisco Unified Communications Manager programming and application development.

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)SU3
- Readme File for Cisco Unified CM IM and Presence Service, Release 11.5(1)SU3a



CHAPTER 2

Upgrades

Upgrade Procedures

Note If your pre-upgrade version is Release 11.5(1)SU8 of Cisco Unified Communications Manager and the IM and Presence Service, you cannot upgrade to Releases 12.0(x), 12.5(1), or 12.5(1)SU1. The minimum Release that you can upgrade to is 12.5(1)SU2.

For detailed procedures on how to upgrade your system, see 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.

Version Requirements

All servers in a Cisco Unified Communications Manager cluster must run the same release. The only exception is during a cluster software upgrade, during which a temporary mismatch is allowed.

The following software versions are supported with Release 11.5(1)SU3:

- Cisco Unified Communications Manager 11.5.1.13902-2 (11.5(1)SU3b)
- Cisco Unified Communications Manager 11.5.1.13901-3 (11.5(1)SU3a)
- Cisco Unified Communications Manager 11.5.1.13900-52 (11.5(1)SU3)
- IM and Presence Service 11.5.1.13900-57

Version Mismatch Not Supported

For your 11.5(1)SU3 deployment to be supported, both Cisco Unified Communications Manager and IM and Presence Service must be running 11.5(1)SU3 versions. Running an 11.5(1)SU3 version of Cisco Unified Communications Manager with an earlier version of IM and Presence Service is not supported. Similarly, running an 11.5(1)SU3 version of IM and Presence Service with an earlier version of Cisco Unified Communications Manager is not supported.

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

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)
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 9 for more information.	11.5(x)	PCD Migration PCD Upgrade (Direct Standard) Cisco Unified OS Admin (Direct Standard)

From	To	Supported Method
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)
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, SU6, SU7, SU8, and SU9 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, Unified Communications Manager cannot synchronize its license usage with the standalone Prime License Manager.

If you are upgrading to one of these 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 Unified Communications Manager.

Note With co-resident Prime License Manager deployments, 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

The following table lists all the phone models that are deprecated for this release of Cisco Unified Communications Manager, along with the Unified CM release where the phone model first became deprecated. For example, a phone model that was first deprecated in Release 11.5(1) is deprecated for all later releases, including all 12.x releases.

If you are upgrading to the current release of Cisco Unified Communications Manager and you have any of these phone models deployed, the phone will not work after the upgrade.

Table 10: Deprecated Phone Models for this Release

Deprecated Phone Models for this Release	First Deprecated as of Unified CM...
• Cisco IP Phone 12 S • Cisco IP Phone 12 SP • Cisco IP Phone 12 SP+ • Cisco IP Phone 30 SP+ • Cisco IP Phone 30 VIP • Cisco Unified IP Phone 7902G • Cisco Unified IP Phone 7905G • Cisco Unified IP Phone 7910 • Cisco Unified IP Phone 7910G • Cisco Unified IP Phone 7910+SW • Cisco Unified IP Phone 7910G+SW • Cisco Unified IP Phone 7912G • Cisco Unified Wireless IP Phone 7920 • Cisco Unified IP Conference Station 7935	11.5(1) and later releases

For additional information, refer to *Field Notice: Cisco Unified Communications Manager Release 11.5(x) does not support some deprecated phone models* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/rel_notes/11_5_1/fieldNotice/cucm_b_fn-deprecated-phone-models-1151.html.

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 this release.
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: https://www.unifiedfx.com/products/unifiedfx-migrationfx#endpoint_refresh_tool.
5. Once all the phones in your network are supported by this release, upgrade your system.

Note Deprecated phones can also be removed after the upgrade. When the administrator logs in to 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 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.

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. See your ISO Readme file for details on your specific ISO file. For-up-to date information on this limitation, see CSCvb14399.

Rolling Back to Previous Versions

If you run into any upgrade issues and you need to roll back to a previous version, you must roll back both the 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 to roll back the Unified Communications Manager version and leave the IM and Presence Service version at 11.5(1)SU3. Similarly, it's not supported to roll back the IM and Presence Service version and leave the Unified Communications Manager version at 11.5(1)SU3.

Upgrading with FIPS Mode Enabled

For Release 11.5(x), 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 Unified Communications Manager in mixed mode. If you are upgrading from an earlier release of 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 following 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. We recommend 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 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 11: 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, see the Cisco Unified Communications Solutions Ordering Guide. **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.
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 12:

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"—See 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:

a. From Cisco Unified CM Administration, choose **Advanced Features** > **Cisco Cloud Onboarding**.

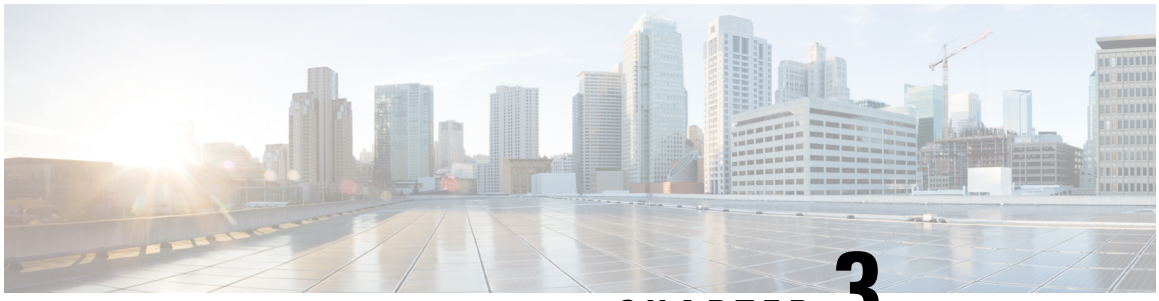
b. Uncheck the following check boxes:

- **Enable Push Notifications**
- **Send Troubleshooting information to the Cisco Cloud**
- **Send encrypted PII to the Cisco Cloud for troubleshooting**

c. 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 guide.



CHAPTER 3

New and Changed Features

Authenticated Network Time Protocol Support

With this release, the authenticated Network Time Protocol (NTP) capability for Cisco Unified Communications Manager is supported. This support is added to secure the NTP server connection to Cisco Unified Communications Manager. In the previous releases, the Cisco Unified Communications Manager connection to the NTP server was not secure.

This feature is based on symmetric key-based authentication and is supported by NTPv3 and NTPv4 servers. Cisco Unified Communications Manager supports only SHA1-based encryption. The SHA1-based symmetric key support is available from NTP version 4.2.6 and above.

- Symmetric Key
- No Authentication

You can check the authentication status of the NTP servers through administration CLI or **NTP Server List** page of the **Cisco Unified OS Administration** application.

CLI Updates for Authenticated NTP

For the authenticated NTP support feature, the following new CLI command is added for this release:

- `utils ntp auth symmetric-key`—This command helps you enable or disable authentication of the selected NTP server. The authentication is based on symmetric keyID and key. The symmetric key is stored in the encrypted format in Cisco UnifiedCommunications Manager.

OS Administration Online Help Updates

Following column has been added in the **NTP Server List** page of the Cisco Unified Operating System Administration application.

NTP Servers Settings

Table 13: NTP Server Configuration Settings

Field	Description
NTP Authentication Status	Displays the authentication status of an NTP server.

Cisco Spark Remote Device

The Cisco Spark Remote Device (Cisco Spark-RD) is a dedicated and fully compatible virtual device for Hybrid Calling's functional requirements and behaviors. Cisco Spark-RD provides the following features:

- Remote Destination (Cisco Webex SIP address) length can be greater than 48 characters.
- Does not require an MTP for calls.
- Does not require IOS-MTP passthrough for video or screen share capability.
- A standalone Cisco Spark-RD uses one Enhanced UCL. If a user has any other UC device that requires an Enhanced UCL, then Cisco Spark-RD does not count towards the license total.

For more information about Cisco Spark-RDs and supported configuration for Hybrid Calling, see http://www.cisco.com/go/hybrid-services-call.

Calendar Integration with Office 365

With this release, you can integrate the IM and Presence Service with an Office 365 server for Microsoft Outlook calendar integration. This configuration allows the IM and Presence Service to pull user calendar information from an Office 365-hosted Microsoft Outlook and display it as a part of a user's presence status. If the user's Outlook calendar indicates that the user is in a meeting, that status gets pulled through and displays in the user's presence status.

This integration has been tested successfully with 15,000 IM and Presence users system, where 5,000 users have a meeting at the top of the hour.

For configuration details, refer to the document *Microsoft Outlook Calendar Integration with the IM and Presence Service*.

User Interface Updates

To support this feature, the **Presence Gateway Settings** window has been updated as follows

- The **Presence Gateway Type** field includes a new gateway option: **Office 365 Server**.
- The following HTTP Proxy fields are added: (**HTTP Proxy URL**, **HTTP Proxy Username**, and **HTTP Proxy Password**). An HTTP Proxy is required if the IM and Presence Service can't access the Office 365 server directly.

New Service Parameter

A new service parameter, **Office365 Calendar Information Pull Interval**, has been added for configuring the PULL interval with an Office 365 server. The IM and Presence Service is not currently able to pull calender information on an ad hoc basis. It can only pull calendar information at regularly scheduled intervals, as configured with this service parameter, which has a default setting of 60 minutes. Make sure to schedule an interval that meets your deployment needs.

Calendaring Troubleshooter

The Calendaring Troubleshooter portion of the System Troubleshooter (**Diagnostics** > **System Troubleshooter**) has been updated for Office 365 integration. When the IM and Presence Service is integrating with an Office 365 server, the troubleshooter confirms that the presence gateway is properly configured, and is reachable.

Cisco Jabber Authentication via OAuth Refresh Logins

Cisco Jabber clients, as of Jabber Release 11.9, can use OAuth Refresh Logins to authenticate with Cisco Unified Communications Manager and the IM and Presence Service. This feature improves the user experience for Cisco Jabber by providing the following benefits:

- After an initial login, provides seamless access to resources over the life of the refresh token.
- Removes the need for Cisco Jabber clients to re-authenticate frequently.
- Provides consistent login behavior in SSO and non-SSO environments.

With OAuth Refresh Logins, Cisco Unified Communications Manager issues clusterwide access tokens and refresh tokens that use the OAuth standard. Cisco Unified Communications Manager and IM and Presence Service use the short-lived access tokens to authenticate Jabber (the default lifespan for an access token is 60 minutes). The longer-lived refresh tokens provide Jabber with new access tokens as the old access tokens expire. So long as the refresh token is valid the Jabber client can obtain new access tokens dynamically without the user having to re-enter credentials (the default refresh token lifespan is 60 days).

All access tokens are encrypted, signed, and self-contained using the JWT format (RFC7519). Refresh tokens are signed, but are not encrypted.

Note OAuth authentication is also supported by Cisco Expressway and Cisco Unified Connection. Make sure to check with those products for compatible versions. Refer to Cisco Jabber documentation for details on Jabber behavior if you are running incompatible versions.

Authentication Process

When a Cisco Jabber client authenticates, or when a refresh token is sent, Cisco Unified Communications Manager checks the following conditions, each of which must be met for authentication to succeed.

- Verifies the signature.
- Decrypts and verifies the token.
- Verifies that the user is an active user. For example, an LDAP-synced user whom is subsequently removed from the external LDAP directory, will remain in the database, but will appear as an inactive user in the User Status of End User Configuration.
- Verifies that the user has access to resources, as provided by their role, access control group, and user rank configuration.

Note For backward compatibility, older Jabber clients and supporting applications such as the Cisco Unified Real-Time Monitoring Tool can authenticate using the implicit grant flow model, which is enabled by default.

Enterprise Parameter Updates

To support this feature, the following enterprise parameters are added under the **SSO and OAuth Configuration** heading:

- **OAuth with Refresh Login Flow**—This parameter controls the login flow used by clients such as Jabber when connecting to Unified CM. OAuth with Refresh Login Flow "enabled" allows the client to use an oAuth-based Fast Login flow to provide a quicker and streamlined login experience, without requiring user input to re-log in (such as after a network change). The option requires support from the other components of the Unified Communications solution, such as Expressway and Unity Connection (compatible versions with refresh login flow enabled). The OAuth with Refresh Login Flow "disabled" option preserves existing behavior and is compatible with older versions of other system components. Note: For Mobile and Remote Access deployment with Jabber, It is recommended to enable this parameter only with a compatible version of Expressway which supports oAuth with Refresh login flow. Incompatible version may impact Jabber functionality. See the specific product documents for supported version and configuration requirements.
- **OAuth Refresh Token Expiry Timer (days)**— This parameter determines the OAuth Refresh token expiry timer in days. Updates to this parameter take effect immediately and refresh tokens issued after the change will use the new expiry timer and previously issued refresh tokens will cease to be valid.

Certificate Updates

To support this feature, the self-signed **AUTHZ** certificate has been added to handle authentication with OAuth tokens. This certificate lives on the Cisco Unified Communications Manager publisher node and replicates the signing and encryption keys to all Cisco Unified Communications Manager and IM and Presence Service cluster nodes. The certificate is self-signed, using a locally-generated public-private key pair and should not be an X.509 certificate.

If you think that either the signing key or encryption key has been compromised, you can regenerate either set of keys. Make sure to sync your new keys with Cisco Expressway and Cisco Unity Connection.

CLI Updates

To support this feature, the following CLI commands are new for this release:

- `set key regen authz signing`—Run this command on the Cisco Unified Communications Manager publisher node to regenerate the asymmetric RSA key pair for signing OAuth access tokens and refresh tokens.
- `set key regen authz encryption`—Run this command on the Cisco Unified Communications Manager publisher node to regenerate the symmetric encryption key that encrypts OAuth access tokens and refresh tokens.
- `show key authz signing`—This command displays the OAuth refresh login encryption key checksum and last synced time on both publisher and subscriber nodes.
- `show key authz encryption`—This command displays the OAuth refresh login signing key checksum and last synced time on both publisher and subscriber nodes.

Troubleshooting

The following table highlights useful logs for troubleshooting OAuth SSO configuration. Trace does not need to be configured for these logs.

Note To set SAML SSO logs to a detailed level, run the `set samltrace level debug` CLI command.

Table 14: Logs for Troubleshooting OAuth Refresh Logins

Logs	Log Details
SSO Logs	Each time a new SSO App operation is completed, new log entries are generated here: `/var/log/active/platform/log/ssoApp.log`
Ssosp Logs	SSO and OAuth operations are logged in ssosp logs. Each time SSO is enabled a new log file is created here: `/usr/local/thirdparty/Jakarta-tomcat/logs/ssosp/log4j/`
SSO and OAuth Configuration	Certificate logs are located at the following location. Each time the Authz certificate is regenerated, a new log file is generated: `/var/log/active/platform/log/certMgmt*.log`

Configure Refresh Logins for Cisco Jabber

Use this procedure to enable Refresh Logins with OAuth access tokens and refresh tokens in Unified Communications Manager. OAuth Refresh Logins provides a streamlined login flow that doesn't require users to re-login after network changes.

Note To ensure compatibility, make sure that the various Unified Communications components of your deployment, such as Cisco Jabber, Cisco Expressway and Cisco Unity Connection, support refresh logins. Once OAuth Refresh Logins are enabled, disabling the feature will require you to reset all Cisco Jabber clients.

Before you begin

You must be running a minimum release of Cisco Jabber 11.9. Older versions of Jabber will use the Implicit Grant Flow authentication model from previous releases.

Procedure

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

Step 2 Under **SSO Configuration**, do either of the following:

- Choose the **OAuth with Refresh Login Flow** enterprise parameter to **Enabled** to enable OAuth Refresh Logins.
- Choose the **OAuth with Refresh Login Flow** enterprise parameter to **Disabled** to disable OAuth Refresh Logins. This is the default setting.

Step 3 If you enabled OAuth Refresh Logins, configure expiry timers for access tokens and refresh tokens by configuring the following enterprise parameters:

- **OAuth Access Token Expiry Timer (minutes)**—This parameter specifies the expiry timer, in minutes, for individual OAuth access tokens. The OAuth access token is invalid after the timer expires, but the Jabber client can request and obtain new access tokens without the user having to re-authenticate so long as the refresh token is valid. The valid range is from 1 - 1440 minutes with a default of 60 minutes.
- **OAuth Refresh Token Expiry Timer (days)**—This parameter specifies the expiry timer, in days, for OAuth refresh tokens. After the timer expires, the refresh token becomes invalid and the Jabber client must re-authenticate to get a new refresh token. The valid range is from 1 - 365 days with a default of 60 days.

Step 4 Click **Save**.

Note Once you've saved the configuration, reset all Cisco Jabber and Webex clients.

Regenerate Keys for OAuth Refresh Logins

Use this procedure to regenerate both the encryption key and the signing key using the Command Line Interface. Complete this task only if the encryption key or signing key that Cisco Jabber uses for OAuth authentication with Unified Communications Manager has been compromised. The signing key is asymmetric and RSA-based whereas the encryption key is a symmetric key.

After you complete this task, the current access and refresh tokens that use these keys become invalid.

We recommend that you complete this task during off-hours to minimize the impact to end users.

The encryption key can be regenerated only via the CLI below, but you can also use the Cisco Unified OS Administration GUI of the publisher to regenerate the signing key. Choose **Security** > **Certificate Management**, select the**AUTHZ** certificate, and click **Regenerate**.

Procedure

Step 1 From the Unified Communications Manager publisher node, log in to the **Command Line** Interface .

Step 2 If you want to regenerate the encryption key:

a) Run the `set key regen authz encryption` command.

b) Enter `yes`.

Step 3 If you want to regenerate the signing key:

a) Run the `set key regen authz signing` command.

b) Enter `yes`.
The Unified Communications Manager publisher node regenerates keys and replicates the new keys to all Unified Communications Manager cluster nodes, including any local IM and Presence Service nodes.

You must regenerate and sync your new keys on all of your UC clusters:

- IM and Presence central cluster—If you have an IM and Presence centralized deployment, your IM and Presence nodes are running on a separate cluster from your telephony. In this case, repeat this procedure on the Unified Communications Manager publisher node of the IM and Presence Service central cluster.
- Cisco Expressway or Cisco Unity Connection—Regenerate the keys on those clusters as well. See your Cisco Expressway and Cisco Unity Connection documentation for details.

Revoke Existing OAuth Refresh Tokens

Use an AXL API to revoke existing OAuth refresh tokens. For example, if an employee leaves your company, you can use this API to revoke that employee's current refresh token so that they cannot obtain new access tokens and will no longer be able to log in to the company account. The API is a REST-based API that is protected by AXL credentials. You can use any command-line tool to invoke the API. The following command provides an example of a cURL command that can be used to revoke a refresh token:

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

where:

- `admin:password` is the login ID and password for the Cisco Unified Communications Manager administrator account.
- `UCMaddress` is the FQDN or IP address of the Cisco Unified Communications Manger publisher node.
- `end_user` is the user ID for the user for whom you want to revoke refresh tokens.

Compliance to Common Criteria

With Release 11.5(1) SU3, both Cisco Unified Communications Manager and IM and Presence Service can run in Common Criteria mode. This running mode runs on a FIPS-enabled system, and allows the system to comply with Common Criteria guidelines.

Common Criteria mode can be configured by running the following CLI commands on each cluster node:

- `utils fips_common_criteria enable` - Run this command to turn Common Criteria mode on.
- `utils fips_common_criteria disable` - Run this command to turn off Common Criteria mode.
- `utils fips_common_criteria status` - Run this command to confirm whether Common Criteria mode is on or off for a particular cluster node.

TLS connection between the MS SQL external database server and the IM and Presence Service server is not supported when Common Criteria mode is enabled on the IM and Presence Service server.

Emergency Notifications Paging

With this release, Cisco Unified Communications Manager comes with a provisioning wizard that allows you to quickly provision and configure advanced notification services.

The Cisco Paging Server product is offered through InformaCast Virtual Appliance. It is a software solution that transforms devices on your network into a powerful system for IP paging and emergency call alerting. It integrates easily with Cisco phones, overhead speakers, strobes, panic buttons, and more, to increase the speed, reach, and success rate of your emergency alerts.

User Interface Updates for Advanced Notification Services

In the **Advanced Features** menu of the Cisco Unified Communications Manager Administration, the **Emergency Notifications Paging** wizard has been added. **Emergency Notifications Paging** is a full-featured emergency notification and paging solution that allows you to reach an unlimited number of Cisco IP phones and various devices and systems with text and audio messages. It includes the following features:

- InformaCast advanced notification
- Panic button configuration
- Text and audio notification to IP phones when a user dials an emergency services number (CallAware)

For more information about InformaCast Virtual Appliance, see https://www.singlewire.com/informacast.html.

Advanced Notification Paging Configuration Task Flow

Perform the following tasks to integrate InformaCast Paging Server with Unified Communications Manager for IP paging and emergency call alerting. It includes the following features:

- InformaCast advanced notification
- Panic button configuration
- Text and audio notification to IP phones when a user dials an emergency services number (CallAware)

Procedure

	Command or Action	Purpose
Step 1	Install the InformaCast Virtual Appliance, on page 27.	Download the InformaCast OVA file from the Singlewire website and upload it to vSphere.
Step 2	Configure Connection to InformaCast, on page 29.	Configure Unified Communications Manager and InformaCast.
Step 3	Configure Panic Button, on page 30.	Configure a panic button to send a text and audio notification to IP phones.
Step 4	Configure CallAware Emergency Call Alerting, on page 31.	Configure emergency call text and audio notifications.

Install the InformaCast Virtual Appliance

Singlewire supports InformaCast Virtual Appliance on the VMware ESXi platform, which is managed through the vSphere client.

Note To view a list of Singlewire-supported VMware ESXi versions, go to this URL: https://www.singlewire.com/compatibility-matrix and click the Server Platforms link under InformaCast Platform section.

Note If you have purchased a license, refer to https://www.singlewire.com/icva-kb-activate to activate your license. This will ensure that Emergency Notifications stay active after the 90-day trial.

Note For more details on the installation, including InformaCast screen captures, go to this URL: https://www.singlewire.com/icva-kb-install.

Before you begin

Import InformaCast Virtual Appliance using the vSphere client. This can be downloaded from your VMware server.

Procedure

Step 1 Download the OVA file from the Singlewire website and then log in to the vSphere client.

Note If you are using InformaCast on the Communications Manager Business Edition 6000, you are supplied with a DVD in a package with an OVA on it (physical media).

The **vSphere Client** window appears.

Step 2 From the **vSphere Client** window, choose **File** > **Deploy OVF Template**.

The **Deploy OVF Template** dialog box appears.

Step 3 Click the **Deploy from File** radio button and then click **Browse** to select the saved the OVA file (or to the OVA file on the supplied DVD). After you select the OVA file, click **Open**.
The **Source** location is selected in the **Deploy OVF Template** dialog box.

Step 4 Click **Next** to continue.
The **Deploy OVF Template** dialog box refreshes and **OVF Template Details** appears.

Step 5 Click **Next** to verify the **Name and Location**, and then click **Next** to select the network to store the new virtual machine files.

Tip It is good practice to place the Virtual Appliance on the same VLAN as your Cisco Unified Communications Manager.

Step 6 Click **Next** to continue, and then click **Finish**.
The InformaCast Virtual Appliance begins importing.

Step 7 From the **vSphere Client** window, click **Hosts and Clusters** icon and then select your host server.
The **vSphere Client** window refreshes.

Step 8 Click the **Configuration** tab and select the **Virtual Machine Startup/Shutdown** link in the **Software** section.

Step 9 Click the **Properties** link.
The **Virtual Machine Startup and Shutdown** dialog box appears.

Step 10 Check the **Allow virtual machines to start and stop automatically with the system** check box under **System Settings**.

Step 11 Under **Startup Order**, scroll to the **Manual Startup** section and select your virtual machine (by default, this is Singlewire InformaCast VM), and then move it from the **Manual Startup** section to the **Automatic Startup** section, by using the **Move Up** button. After moving it, click **OK**.
The InformaCast Virtual Appliance starts and stops automatically with the server on which it is hosted. Now you can turn on InformaCast's virtual machine and set its network configuration.

Step 12 Choose **View** > **Inventory** > **VMs and Templates** and then select your virtual machine.

Step 13 Choose the **Inventory** > **Virtual Machine** > **Open Console**
The Singlewire InformaCast VM console window appears.

Step 14 InformaCast configuration starts for the first time. During this configuration, perform the following tasks for the InformaCast Virtual Appliance:

a) Accept Cisco End User License Agreement (EULA)
b) Accept Singlewire EULA
c) Set up hostname
d) Set up IP address, subnet mask, and default gateway
e) Set up DNS server IP address and domain name
f) Set up NTP server IP address or hostname
g) Set up time zone
h) Set up Secure Socket Layer (SSL) certificate parameters
i) Set up SSL subject alternate names (optional)
j) Set up the OS admin password
k) Set up the InformaCast and PTT (PushToTalk) admin password. This password is required to connect the Cisco Unified Communications Manager and InformaCast in the Cisco Unified CM Administration, **Advanced Features** > **Emergency Notifications Paging**.
l) Set up security passphrase for backup and communication

When your configuration is successful, the “Welcome to Singlewire InformaCast” message is displayed.

Step 15 Click **Continue** to work with Singlewire InformaCast.

Configure Connection to InformaCast

Use this procedure to load the InformaCast certificate to the Unified Communications Manager Tomcat trust store.

Before you begin

Install the InformaCast Virtual Appliance, on page 27.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **Emergency Notifications Paging**.

Step 2 In the **Introduction to InformaCast Emergency Notifications** page, click **Next** to continue.
The **Installing the InformaCast Virtual Appliance** page appears.

Step 3 In the **Installing the InformaCast Virtual Appliance** page, click **Next** to continue.

Note You should have successfully installed InformaCast Virtual Appliance to configure with the Unified Communications Manager.

The **Connecting Cisco Unified Communications Manager and InformaCast** page appears.

Step 4 In the **IP address of InformaCast VM** field, enter either IP address or Hostname.

Note By default, the username is stated as `admin` in the **Username to use in InformaCast** field, and it is not editable.

Step 5 In the **Password for admin app user** field, enter the administrator password of the InformaCast application.
The dialog box displaying the thumbprint of InformaCast certificate is displayed.

Step 6 Click **OK** to load the InformaCast certificate to the Unified Communications Manager Tomcat trust store.
Configuration process starts.

Note When the configuration is successful, the **Status** field displays the completion status.

Step 7 Click **Next**.
The wizard performs the following tasks:

- Activates SNMP service
- Configures SNMP Service with locally generated random credentials
- Activates CTI Manager Service
- Configures Unified Communications Manager for InformaCast
    - Creates new region (1 per cluster)
    - Creates new device pool (1 per cluster)
    - Creates SIP trunk (1 per cluster)
    - Creates route group (1 per cluster)

- Creates route list
- Creates role
- Creates app user

- Configures InformaCast for Unified Communications Manager
  - Creates a cluster
  - Refreshes recipient groups
  - Sets SIP access to deny
  - Creates SIP access

Configure Panic Button

Use this procedure to configure a panic button to send a text and audio notification to IP phones. This allows you to initiate a one click alarm if there is emergency.

Before you begin

Configure Connection to InformaCast, on page 29.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **Emergency Notifications Paging**.

Step 2 In the **Introduction to InformaCast Emergency Notifications** page, click **Next** to continue.

Step 3 In the **Installing the InformaCast Virtual Appliance** page, click **Next** to continue.

Step 4 In the **Connecting Cisco Unified Communications Manager and InformaCast** page, click **Next** to continue. The **Configuring a Panic Button** page appears.

Step 5 From the **Choose pre-recorded message by name** drop-down list, select the pre-recorded message to be displayed on Cisco Unified IP phones and various devices and systems in emergency.

Note You can change the pre-recorded message in InformaCast administration, as required.

Step 6 In the **Enter DN to trigger the panic button** field, enter the Directory Number (DN), which includes the digits 0 to 9, asterisks (*), and pound signs (#). Default value is ***5.

Step 7 From the **Route Partition** drop-down list, select a partition to restrict access to the route pattern.

Note If you do not want to restrict access to the route pattern, select <None> for the partition.

Step 8 Click **Choose Phones to Send Notification** button.
The **Phones to Send Notification** dialog box appears.

Step 9 From the **Phones to Send Notification** dialog box, select the Cisco Unified IP phones to send the pre-recorded message. The dial pattern entered by you (for example, ***5) is configured as speed dial on the selected phones.
The selected Cisco Unified IP Phone are displayed in the **Selected Phones to Send Notification** list box.

Step 10 Click **Add Rules**, to create a new rule for the selected Cisco Unified IP Phone to receive notifications.

a) Select one of the parameters from the drop-down list. The available options are Device Pool, Description, and Directory Number.

b) In the second drop-down list, select a criteria from the following options:

- Does
- Does not

c) In the third drop-down list, select a criteria from the following options:

- Begins with
- Ends with
- Contains

d) In the text box, enter the search criterion.

Note Minimum of one new rule and maximum of new five rules can be created. The **Add Rules** button gets disabled when five rules are created.

Note To delete a rule, click **Delete Rules**.

e) Click **Test Rules**, to validate the created rules. When the test rule is completed with more than zero phones, the **Next** button is enabled.

Note Phones added to Cisco Unified Communications Manager at a later date that match this rule will be included as recipients in notifications to this group.

Step 11 Click **Next**.

The wizard performs the following tasks:

- Adds a speed dial for the entered DN to the selected phones. If the selected phones have unused speed dials assigned to existing phone button templates, this speed dial appears directly on the selected phones. If the selected phones do not have unused speed dial buttons, the panic button speed dial is created, but it does not appear on the phone.
- Adds route pattern for entered DN in selected partition using created route list.
- Creates an InformaCast DialCast entry for the entered DN to send the selected message to the phones matching the selected rules.

Configure CallAware Emergency Call Alerting

Use this procedure to configure the CallAware emergency call alerting details. This sends a text and audio notification to IP phones when an emergency number is dialed. It can also detect calls to numbers other than 911.

Before you begin

Configure Panic Button, on page 30.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **Emergency Notifications Paging**.

Step 2 In the **Introduction to InformaCast Emergency Notifications** page, click **Next** to continue.

Step 3 In the **Installing the InformaCast Virtual Appliance** page, click **Next** to continue.

Step 4 In the **Connecting Cisco Unified Communications Manager and InformaCast** page, click **Next** to continue.

Step 5 In the **Configuring a Panic Button** page, click **Next** to continue.
The **Configuring CallAware Emergency Call Alerting** page appears.

Step 6 From the **Choose pre-recorded message by name** drop-down list, select the pre-recorded message to be displayed on Cisco Unified IP phones and various devices and systems in emergency.

Note You can change the pre-recorded message in InformaCast administration, as required.

Step 7 Click **Choose Emergency Route Patterns** button.
The **Route Patterns** dialog box appears.

Step 8 From the **Route Patterns** dialog box, select the route patterns by checking the box next to the desired patterns.

a) Click the **Save Selected/Changes** button.

The selected route patterns are displayed in the **Selected Route Patterns** list box.

Step 9 Click **Add Rules**, to create a new rule for the selected Cisco Unified IP Phone to receive notifications.

a) Select one of the parameters from the drop-down list. The available options are Device Pool, Description, and Directory Number.

b) In the second drop-down list, select a criteria from the following options:

- Does
- Does not

c) In the third drop-down list, select a criteria from the following options:

- Begins with
- Ends with
- Contains

d) In the text box, enter the search criterion.

Note Minimum of one new rule and maximum of five new rules can be created. The **Add Rules** button gets disabled when five rules are created.

Note To delete a rule, click **Delete Rules**.

e) Click **Test Rules**, to validate the created rules. When the test rule is completed with more than zero phones, the **Finish** button is enabled.

Note Phones added to Unified Communications Manager at a later date that match this rule will be included as recipients in notifications to this group.

Step 10 Click **Finish**.

The wizard performs the following tasks:

- Adds External Call Control profile for InformaCast
- For each selected route pattern, modify that route pattern to reference the External Call Control profile
- Creates a recipient group with rules that match phones to receive the notification
- Creates an InformaCast routing request with the selected message and recipient group

The **Summary** page appears and confirms the successful configuration of InformaCast with Unified Communications Manager. For more information, see https://www.singlewire.com.

Paging Interactions

• Advanced Notification Paging Interactions, on page 33

Advanced Notification Paging Interactions

Table 15: Advanced Notification Paging Interactions

Feature	Interaction
Emergency Notifications Paging	You can configure the Emergency Notifications Paging wizard using InformaCast Release 11.5(1)SU3 and later versions in basic paging mode only. You can configure call monitoring to route patterns that contain digits only in the Emergency Notifications Paging wizard. For route patterns that contain wildcard characters, configure in InformaCast.

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 following 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 16: 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, see the Cisco Unified Communications Solutions Ordering Guide. **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.
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*.

Enhanced Sign-In Experience for Cisco Jabber During SSO and Non-SSO

From this release, the sign-in experience for Cisco Jabber will be similar for Single Sign-On (SSO) and non-SSO. The refresh token feature enhances the Jabber user experience across devices and especially for Jabber on Mobile. The login flow for Jabber non-SSO is now similar to Jabber SSO . An end user can now sign-in by generating an OAuth code, which in turn generates an access token and a refresh token to enable logging in to Jabber. When an access token expires, the refresh token is used to generate the access token. This prevents the login flow from being repeated and enhances performance during Jabber sign-in.

Cisco Jabber Client version 11.9.0 supports the refresh token feature.

Enhanced Usability in the User Device Association Screen

The **User Device Association** screen allows administrators to associate or disassociate devices with end users and application users. As of Release 115.1 SU3, the user interface of the **User Device Association** screen has been enhanced to ensure that an admin is sure about working on the selected user. The **Remove All Associated Devices** button has been realigned on the UI to prevent an admin from unintentionally removing devices associated with a user.

User Interface Updates

- The User ID of the selected user is displayed in the **User Device Association** screen. The following labels have been updated:
  - The name of the section **User Device Association** is now updated to **User Device Association For <User ID>**.
  - The name of the check box **Show the devices already associated** is now updated to **Show the devices already associated with <User ID>**.
- The **Remove All Associated Devices** button is now available at the right corner of the toolbar to distinguish it from other toolbar buttons.
- The confirmation message displayed on clicking the **Remove All Associated Devices** button now specifies the user ID and number of devices selected for disassociation.
- The **Remove All Associated Devices** button is not displayed when the filter is applied. This ensures that an admin does not unintentionally disassociate all the associated devices.

Minimum TLS Version Control

This release of Cisco Unified Communications Manager and IM and Presence Services includes the minimum Transport Layer Security (TLS) protocol version configuration support. Use this feature to configure the minimum TLS version to comply with the organization security policies.

The supported TLS versions are TLS 1.0, 1.1, and 1.2. By default, TLS 1.0 is configured. After you configure the minimum TLS version, both the minimum version and the higher versions are supported.

Before you configure the minimum TLS version, ensure that the following products support secure connection of the selected minimum TLS version configured or above with Cisco Unified Communications Manager and IM and Presence Services. If this requirement is not met, upgrade the product to a version that supports the interoperability for selected minimum TLS version configured or above when you configure the minimum TLS version.

- Skinny Client Control Protocol (SCCP) Conference Bridge
- Transcoder
- Hardware Media Termination Point (MTP)
- SIP Gateway
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment
- Cisco Unified Border Element (CUBE)
- Cisco Expressway
- Cisco TelePresence Conductor

Note

- This feature is implemented at Command Line Interface and is applicable to both Cisco Unified Communications Manager and IM and Presence Services.
- Cisco Unified Communications Manager and IM and Presence Services Release 9.x and below do not support TLS 1.1 and above. Hence, before you proceed for interoperability of these applications of Release 9.x with Cisco Unified Communications Manager and IM and Presence Services of Release 11.5(1)SU3 and above, configure minimum TLS version as 1.0. This configuration is required for functions, such as Extensible Messaging and Presence Protocol (XMPP) federation deployment, Extension Mobility Cross Cluster (EMCC), Inter Cluster Sync Agent (ICSA), and SIP Trunk functionality that do not support TLS 1.1 and above.
- You can enable Common Criteria mode along with configuration of minimum TLS version. If you do so, the applications continue to comply with Common Criteria requirements and disable TLS 1.0 secure connections at application level. When the common criteria mode is enabled, you can configure the minimum TLS version as either 1.1 or 1.2 for the applications. If you try to configure the minimum TLS version as 1.0, an error appears at Command Line Interface. For details on Common Criteria mode, see the Compliance to Common Criteria topic of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

To configure the minimum TLS version, see the CLI Commands for Minimum TLS Version, on page 36 topic.

CLI Commands for Minimum TLS Version

For the minimum TLS version feature, the following new CLI commands are added for this release:

- `set tls min-version`—This command sets the minimum version of Transport Layer Security (TLS) protocol.
- `show tls min-version`—This command shows the minimum configured version of Transport Layer Security (TLS) protocol.

For additional information on these CLI commands, see the *Command Line Interface Reference 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 Updates

The new chapter, "TLS Setup", is added to the *Security Guide for Cisco Unified Communications Manager*. The chapter is added to include the Minimum TLS Version Control feature that is introduced with this release. The chapter provides an overview of TLS, its prerequisites, how to configure TLS, and the interactions and restrictions.

TLS Overview

Transport Layer Security (TLS) provides secure and reliable signaling and data transfer between two systems or devices, by using secure ports and certificate exchange. TLS secures and controls connections among Unified Communications Manager-controlled systems, devices, and processes to prevent access to the voice domain.

TLS Prerequisites

Before you configure the minimum TLS version, make sure that your network devices and applications both support the TLS version. Also, make sure that they are enabled for TLS that you want to configure with Unified Communications Manager and IM and Presence Services. If you have any of the following products deployed, confirm that they meet the minimum TLS requirement. If they do not meet this requirement, upgrade those products:

- Skinny Client Control Protocol (SCCP) Conference Bridge
- Transcoder
- Hardware Media Termination Point (MTP)
- SIP Gateway
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment
- Cisco Unified Border Element (CUBE)
- Cisco Expressway
- Cisco TelePresence Conductor

You will not be able to upgrade conference bridges, Media Termination Point (MTP), Xcoder, Prime Collaboration Assurance, and Prime Collaboration Provisioning.

Note If you are upgrading from an earlier release of Unified Communications Manager, make sure that all your devices and applications support the higher version of TLS before you configure it. For example, Unified Communications Manager and IM and Presence Services, Release 9.x supports TLS 1.0 only.

TLS Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	(Optional) Set Minimum TLS Version, on page 38.	By default, Cisco Unified Communications Manager supports a minimum TLS version of 1.0. If your security needs require a higher version of TLS, reconfigure the system to use TLS 1.1 or 1.2.
Step 2	Set TLS Ciphers, on page 39.	Configure an enterprise parameter for the TLS cipher options that Cisco Unified Communications Manager supports.
Step 3	Configure TLS in a SIP Trunk Security Profile, on page 39 .	Assign TLS connections to a SIP Trunk. Trunks that use this profile use TLS for signaling. You can also use the secure trunk to add TLS connections to devices, such as conference bridges.
Step 4	Add Secure Profile to a SIP Trunk, on page 40.	Assign a TLS-enabled SIP trunk security profile to a SIP trunk to allow the trunk to support TLS. You can use the secure trunk to connect resources, such as conference bridges.
Step 5	Configure TLS in a Phone Security Profile, on page 41.	Assign TLS connections to a phone security profile. Phones that use this profile use TLS for signaling.
Step 6	Add Secure Phone Profile to a Phone, on page 41.	Assign the TLS-enabled profile that you created to a phone.
Step 7	(Optional) Add Secure Phone Profile to a Universal Device Template, on page 42.	Assign a TLS-enabled phone security profile to a universal device template. If you have the LDAP directory synchronization configured with this template, you can provision phones with security through the LDAP sync.

Set Minimum TLS Version

By default, Cisco Unified Communications Manager supports a minimum TLS version of 1.0. Use this procedure to reset the minimum supported TLS version for Cisco Unified Communications Manager and the IM and Presence Service to a higher version, such as 1.1 or 1.2.

Before you begin

Make sure that the devices and applications in your network support the TLS version that you want to configure. For details, see TLS Prerequisites, on page 37.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 To confirm the existing TLS version, run the **show tls min-version** CLI command.

Step 3 Run the **set tls min-version** <*minimum*> CLI command where <*minimum*> represents the TLS version.

For example, run **set tls min-version 1.2** to set the minimum TLS version to 1.2.

Step 4 Perform Step 3 on all Cisco Unified Communications Manager and IM and Presence Service cluster nodes.

What to do next

Set TLS Ciphers, on page 39

Set TLS Ciphers

Use this procedure to configure the ciphers that Cisco Unified Communications Manager supports for establishing TLS connections.

Procedure

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

Step 2 In **Security Parameters**, configure a value for the **TLS Ciphers** enterprise parameter. For help on the available options, refer to the enterprise parameter help.

Step 3 Click **Save**.

What to do next

Configure TLS in a SIP Trunk Security Profile, on page 39

Configure TLS in a SIP Trunk Security Profile

Use this procedure to assign TLS connections to a SIP Trunk Security Profile. Trunks that use this profile use TLS for signaling.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **SIP Trunk Security Profile**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new SIP trunk security profile.

- Click **Find** to search and select an existing profile.

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

Step 4 Configure the **Device Security Mode** field value to **Encrypted** or **Authenticated**.

Step 5 Configure both the **Incoming Transport Type** and **Outgoing Transport Type** field values to **TLS**.

Step 6 Complete the remaining fields of the **SIP Trunk Security Profile** window. For help on the fields and their configuration, see the online help.

Step 7 Click **Save**.

What to do next

Add Secure Profile to a SIP Trunk, on page 40

Add Secure Profile to a SIP Trunk

Use this procedure to assign a TLS-enabled SIP trunk security profile to a SIP trunk. You can use this trunk to create a secure connection to resources, such as conference bridges.

Before you begin

Configure TLS in a SIP Trunk Security Profile, on page 39

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new trunk.
- Click **Find** to search and select an existing trunk.

Step 3 If you are creating a new trunk, select the trunk type and protocol, and click **Next**.

Step 4 For the **Device Name** field, enter a device name for the trunk.

Step 5 From the **Device Pool** drop-down list, choose a device pool.

Step 6 From the **SIP Profile** drop-down list, choose a SIP Profile.

Step 7 From the **SIP Trunk Security Profile** drop-down list, choose the TLS-enabled SIP Trunk Profile that you created in the previous task.

Step 8 In the **Destination** area, enter the destination IP address. You can enter up to 16 destination addresses. To enter additional destinations, click the (+) button.

Step 9 Complete the remaining fields in the **Trunk Configuration** window. For help with the fields and their configuration, see the online help.

Step 10 Click **Save**.

Note If you are connecting the trunk to a secure device, you must upload a certificate for the secure device to Cisco Unified Communications Manager. For certificate details, see the “Certificates” topic of *Security Guide for Cisco Unified Communications Manager*.

What to do next

Configure TLS in a Phone Security Profile, on page 41.

Configure TLS in a Phone Security Profile

Use this procedure to assign TLS connections to a Phone Security Profile. Phones that use this profile use TLS for signaling.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new profile.
- Click **Find** to search and select an existing profile.

Step 3 If you are creating a new profile, select a phone model and protocol, and click **Next**.

Note If you want to use a universal device template and LDAP sync to provision security through the LDAP sync, select **Universal Device Template** as the **Phone Security Profile Type**.

Step 4 Enter a name for the profile.

Step 5 From the **Device Security Mode** drop-down list, select either **Encrypted** or **Authenticated**.

Step 6 (For SIP phones only) From the Transport Type, select **TLS**.

Step 7 Complete the remaining fields of the **Phone Security Profile Configuration** window. For help with the fields and their configuration, see the online help.

Step 8 Click **Save**.

Add Secure Phone Profile to a Phone

Use this procedure to assign the TLS-enabled phone security profile to a phone.

Note To assign a secure profile to a large number of phones at once, use the Bulk Administration Tool to reassign the security profile for them.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new phone.
- Click **Find** to search and select an existing phone.

Step 3 Select the phone type and protocol and click **Next**.

Step 4 From the **Device Security Profile** drop-down list, assign the secure profile that you created to the phone.

Step 5 Assign values for the following mandatory fields:

- MAC address
- Device Pool
- SIP Profile
- Owner User ID
- Phone Button Template

Step 6 Complete the remaining fields of the **Phone Configuration** window. For help with the fields and their configuration, see the online help.

Step 7 Click **Save**.

Add Secure Phone Profile to a Universal Device Template

Use this procedure to assign a TLS-enabled phone security profile to a universal device template. If you have LDAP directory sync configured, you can include this universal device template in the LDAP sync through a feature group template and user profile. When the sync occurs, the secure profile is provisioned to the phones.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Universal Device Template**.

Step 2 Perform one of the following steps:

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

Step 3 For the **Name** field, enter a name for the template.

Step 4 From the **Device Pool** drop-down list, select a device pool.

Step 5 From the **Device Security Profile** drop-down list, select the TLS-enabled security profile that you created.

Note The Phone Security Profile must have been created with **Universal Device Template** as the device type.

Step 6 Select a **SIP Profile**.

Step 7 Select a **Phone Button Template**.

Step 8 Complete the remaining fields of the **Universal Device Template Configuration** window. For help with the fields and their configuration, see the online help.

Step 9 Click **Save**.
Include the Universal Device template in an LDAP directory synchronization. For 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.

TLS Interactions and Restrictions

This chapter provides information about the TLS Interactions and Restrictions.

TLS Interactions

Table 17: TLS Interactions

Feature	Interaction
Common Criteria mode	You can enable Common Criteria mode along with configuration of minimum TLS version. If you do so, the applications continue to comply with Common Criteria requirements and disable TLS 1.0 secure connections at application level. When the common criteria mode is enabled, you can configure the minimum TLS version as either 1.1 or 1.2 for the applications. For details on Common Criteria mode, see the Compliance to Common Criteria topic of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

TLS Restrictions

The following table highlights issues that you may run into when implementing Transport Layer Security (TLS) version 1.2 on legacy phones, such as 79xx, 69xx, 89xx, 99xx, 39xx, and IP Communicator. To verify whether your phone supports secure mode in this release, see the Phone Feature List Report in Cisco Unified Reporting. The feature restrictions on legacy phones and the workaround to implement the feature is listed in the following table:

Note The workarounds are designed to get the impacted feature functioning in your system. However, they do not guarantee TLS 1.2 compliance for that feature.

Table 18: Transport Layer Security Version 1.2 Restrictions

Feature	Restriction
Legacy phones in Encrypted Mode	Legacy phones in Encrypted Mode do not work. There is no workaround.
Legacy phones in Authenticated Mode	Legacy phones in Authenticated Mode do not work. There is no workaround.
IP Phone services using secure URLs based on HTTPS.	IP Phone services using secure URLs based on HTTPS do not work. Workaround to use IP Phone services: Use HTTP for all underlying service options. For example, corporate directory and personal directory. However, HTTP is not recommended as HTTP is not as secure if you need to enter sensitive data for features, such as Extension Mobility. The drawbacks of using HTTP include: • Provisioning challenges when configuring HTTP for legacy phones and HTTPS for supported phones. • No resiliency for IP Phone services. • Performance of the server handling IP phone services can be affected.

Feature	Restriction
Extension Mobility Cross Cluster (EMCC) on legacy phones	EMCC is not supported with TLS 1.2 on legacy phones. Workaround: Complete the following tasks to enable EMCC: **1.** Enable EMCC over HTTP instead of HTTPS. **2.** Turn on mixed-mode on all Unified Communications Manager clusters. **3.** Use the same USB eTokens for all Unified Communications Manager clusters.
Locally Significant Certificates (LSC) on legacy phones	LSC is not supported with TLS 1.2 on legacy phones. As a result, 802.1x and phone VPN authentication based on LSC are not available. Workaround for 802.1x: Authentication based on MIC or password with EAP-MD5 on older phones. However, those are not recommended. Workaround for VPN: Use phone VPN authentication based on end-user username and password.
Encrypted Trivial File Transfer Protocol (TFTP) configuration files	Encrypted Trivial File Transfer Protocol (TFTP) configuration files are not supported with TLS 1.2 on legacy phones even with Manufacturer Installed Certificate (MIC). There is no workaround.
CallManager certificate renewal causes legacy phones to lose trust	Legacy phones lose trust when CallManager certificate is renewed. For example, a phone cannot get new configurations after renewing the certificate. This is applicable only in Unified Communications Manager 11.5.1 Workaround: To prevent legacy phones from losing trust, complete the following steps: **1.** Before you enable the CallManager certificate, set the **Cluster For Roll Back to Pre 8.0** enterprise parameter to **True**. By default, this setting disables the security. **2.** Temporarily allow TLS 1.0 (multiple Unified Communications Manager reboots).
Connections to non-supported versions of Cisco Unified Communications Manager	TLS 1.2 connections to older versions of Unified Communications Manager that do not support the higher TLS version do not work. For example, a TLS 1.2 SIP trunk connection to Unified Communications Manager Release 9.x does not work because that release does not support TLS 1.2. You can use one of the following workarounds: • Workaround to enable connections: Use nonsecure trunks, although this is not a recommended option. • Workaround to enable connections while using TLS 1.2: Upgrade the non-supported version to a release that does support TLS 1.2.

Feature	Restriction
Certificate Trust List (CTL) Client	CTL client does not support TLS 1.2. You can use one of the following workarounds: • Temporarily allow TLS 1.0 when using the CTL client and then move the Cluster to Common Criteria mode. Configure Minimum TLS to 1.1 or 1.2 • Migrate to the Tokenless CTL by using the CLI Command **utils ctl set-cluster mixed-mode** in Common Criteria mode. Configure Minimum TLS to 1.1 or 1.2
Address Book Synchronizer	There is no workaround.

Cisco Unified Communications Manager Ports Affected by Transport Layer Security Version 1.2

The following table lists the Unified Communications Manager Ports Affected By TLS Version 1.2

Table 19: Cisco Unified Communications Manager Ports Affected by Transport Layer Security Version 1.2

Application	Protocol	Destination / Listener	Cisco Unified Communications Manager Operating in Normal mode			Cisco Unified Communications Manager Operating in Common Criteria Mode		
			Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2
Tomcat	HTTPS	443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS v1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
SCCP - SEC - SIG	Signalling Connection Control Part (SCCP)	2443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
CTL-SERV	Proprietary	2444	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
Computer Telephony Integration (CTI)	Quick Buffer Encoding (QBE)	2749	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
CAPF-SERV	Transmission Control Protocol (TCP)	3804	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2

Application	Protocol	Destination / Listener	Cisco Unified Communications Manager Operating in Normal mode			Cisco Unified Communications Manager Operating in Common Criteria Mode		
			Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2
Intercluster Lookup Service (ILS)	Not applicable	7501	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
Administrative XML (AXL)	Simple Object Access Protocol (SOAP)	8443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
High Available-Proxy (HA-Proxy)	TCP	9443	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.2	TLS 1.2
SIP-SIG	Session Initiation Protocol (SIP)	5061 (configurable with trunk)	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
HA Proxy	TCP	6971, 6972	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
Cisco Tomcat	HTTPS	8080, 8443	8443: TLS 1.0, TLS 1.1, TLS 1.2	8443: TLS 1.1, TLS 1.2	8443: TLS 1.2	TLS 1.1	8443: TLS 1.1, TLS 1.2	8443: TLS 1.2
Trust Verification Service (TVS)	Proprietary	2445	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2

Instant Messaging and Presence Ports Affected by Transport Layer Security Version 1.2

The following table lists the IM and Presence Service Ports Affected By Transport Layer Security Version 1.2:

Table 20: Instant Messaging & Presence Ports Affected by Transport Layer Security Version 1.2

Destination/Listener	Instant Messaging & Presence Operating in Normal mode			Instant Messaging & Presence Operating in Common Criteria mode		
	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2
443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
5061	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
5062	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
7335	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
8083	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
8443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2

Push Notifications Enhancements for Cisco Jabber on iPhone and iPad

With this release, the Push Notifications for Cisco Jabber on iPhone and iPad solution has been enhanced with the following updates:

- Voice and Video Call Support—Cisco Unified Communications Manager now uses Push Notifications to send voice and video calls to Cisco Jabber on iPhone or iPad clients that are in suspended mode. This update removes the need to use the cellular network to reach Jabber on iPhone and iPad clients that are in suspended mode, thereby decreasing your network costs.
- High Availability for IM and Presence—This release adds failover protection for Push Notifications-enabled IM and Presence sessions over Cisco Jabber on iPhone or iPad. With this feature, the backup node in the subcluster can take over a failed session without a need for any user action. The backup node can completely recreate the IM session so that the user does not lose the IM history.
- Troubleshooting Options—This release provides additional troubleshooting options for troubleshooting and debugging your system. This ensures that your system remains up and running at all times.

For additional detail on the Push Notifications solution with Release 11.5(1)SU3, refer to *Deploying Push Notifications for Cisco Jabber on iPhone and iPad* 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.

User Interface Updates

With this release, the **Enable Push Notifications and Send Troubleshooting and Analytics Information to Cisco Cloud** check box in the **Cisco Cloud Onboarding** window has been replaced with the following new fields:

- **Enable Push Notifications**— Check this check box to enable Push Notifications voice, video and IM and Presence support for Cisco Jabber on iPhone and iPad clients.
- **Send Troubleshooting information to the Cisco cloud**—When the check box is checked, Cisco Unified Communications Manager and IM and Presence Service cluster sends alarm syslog files at regular intervals to the Cisco Cloud. Cisco uses this information for proactive debugging and problem resolution.
- **Send encrypted PII to the Cisco cloud for troubleshooting**—When this check box is checked, Cisco Unified Communications Manager encrypts all troubleshooting data that can be used to identify the partner before sending to the Cisco Cloud (for example, device names or hostnames).

CLI Commands for Troubleshooting Push Notifications

Push Notifications provides the following CLI commands, which can be run on the Unified Communications Manager publisher node for troubleshooting:

- **utils managementAgent alarms pushfrequency**—Run this command to configure the interval following which Cisco Unified Communications Manager sends Push Notifications alarms to the Cisco Cloud. The default value is 30 minutes.
- **utils managementAgent alarms pushlevel**—Run this command to configure the minimum severity level for which Cisco Unified Communications Manager sends Push Notifications alarms to the Cisco Cloud. The default severity is `Error`.
- **utils managementAgent alarms pushnow**—Run this command to upload Push Notifications alarms to the Cisco Cloud immediately, without waiting for the interval to expire.

TLS as a Communication Protocol for Syslog and FileBeat

Cisco Unified Communications Manager and IM and Presence Service will be made Common Criteria compliant from version 11.5.1 SU3 onwards. It is mandatory to use Transport Layer Security (TLS) 1.2 as a communication protocol to comply with Common Criteria guidelines. As of Release 11.5(1) SU2, Transport Layer Security (TLS) 1.2 can be used as a communication protocol for syslog and FileBeat. The TLS 1.2 protocol enables the establishment of a secure connection in the following scenarios:

- Connecting Cisco Unified Communications Manager and IM and Presence Service with syslog servers
- Connecting FileBeat client with external logstash servers

Administrators can configure TLS for remote syslog and FileBeat using CLI commands.

Note

- Ensure that the syslog server supports TLS 1.2 protocol as a secure connection will be established only if the syslog server supports TLS 1.2 protocol.
- In Common Criteria Mode, strict host name verification will be implemented. Hence, it is required to configure the server with a fully qualified domain name (FQDN) which matches the certificate.

New CLI Commands for Protocol Switch

Administrators with privilege level 4 access can configure TLS as the communication protocol using the following CLI commands:

- CLI command for remote syslog communication:

  `utils remotesyslog set protocol tls`- Sets TLS as the communication protocol for connecting Cisco Unified Communications Manager and IM and Presence Service with syslog servers

- CLI commands for FileBeat clients:
  - `utils filebeat tls enable`- Enables a secure connection between the FileBeat client and the logstash server.
  - `utils filebeat tls disable`- Disables the TLS for FileBeat client.
  - `utils filebeat tls status`- Displays the status for TLS.

New Alarms to Indicate Loss of Connection

An alarm `TLSRemoteSyslogDeliveryFailed` with severity `ERROR_ALARM` triggers if the connection between Cisco Unified Communications Manager or IM and Presence Service with syslog servers is lost. An alert Cisco `TLSRemoteSyslogDeliveryFailed` is also sent to RTMT Alert Central.

Upgrade External Database Table Values for Microsoft SQL Datatype

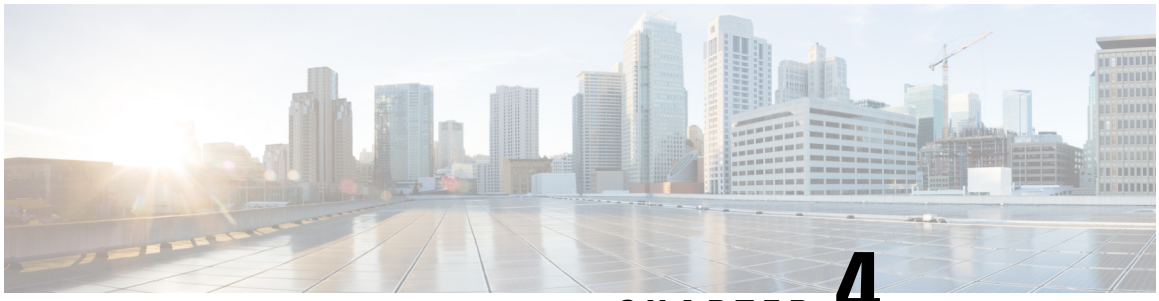
In earlier versions of IM and Presence Service, there was no option to write Unicode characters to a persistent chat room when Microsoft SQL server is configured as external database.

With this release, Microsoft SQL Datatype values are upgraded from text to nvarchar (new size) and varchar (existing size) to nvarchar (existing size) in the following tables:

- AFT_LOG Table
- TC_ROOMS Table
- TC_USERS Table
- TC_MESSAGES Table
- TC_TIMELOG Table
- TC_MSGARCHIVE Table

- JM Table

For detailed information on Microsoft SQL Datatype values, refer to *Database Setup for IM and Presence Service on Cisco Unified Communications Manager, Release 11.5(SU3)*.



CHAPTER 4

Important Notes

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

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 interface by navigating 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).

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.

New Cisco Gateway Support

New releases of Unified Communications Manager have introduced support for the following Cisco gateways:

- Cisco VG400 Analog Voice Gateway
- Cisco VG420 Analog Voice Gateway
- Cisco VG450 Analog Voice Gateway
- Cisco 4461 Integrated Services Router

The following table lists supported gateway models and the initial release, by release category, where support was introduced. Within each release category (e.g., 10.5(2), 11.5(x)), support for the gateway model is added as of the specified release, along with later releases in that category. For these releases, you can select the gateway in the **Gateway Configuration** window of Unified Communications Manager.

Table 21: Cisco Gateways with Initial Release By Release Category

Gateway Model	10.5(2) Releases	11.5(x) Releases	12.0(x) Releases	12.5(x) Releases	14(x) Releases
Cisco VG 202, 202 XM, 204, 204 XM, 310, 320, 350 Analog Voice Gateway	10.5(2) and later	11.5(1) and later	12.0(1) and later	12.5(1) and later	14 and later
Cisco VG400 Analog Voice Gateway	Not supported	11.5(1)SU7 and later	12.0(1)SU2 and later	12.5(1) and later	14 and later
Cisco VG420 Analog Voice Gateway	Not supported	11.5(1)SU9 and later	12.0(1)SU2 and later	12.5(1)SU4 and later	14SU1 and later
Cisco VG450 Analog Voice Gateway	10.5(2)SU8 and later	11.5(1)SU6 and later	12.0(1)SU2 and later	12.5(1) and later	14 and later
Cisco 4321, 4331 4351, 4431, 4451 Integrated Services Router	10.5(2) and later	11.5(1) and later	12.0(1)SU2 and later	12.5(1) and later	14 and later
Cisco 4461 Integrated Services Router	10.5(2)SU8 and later	11.5(1)SU6 and later	12.0(1)SU2 and later	12.5(1) and later	14 and later

Cisco Analog Telephone Adapters

Cisco Analog Telephone Adapters connect analog devices, such as an analog phone or fax machine, to your network. These devices can be configured via the **Phone Configuration** window. The following table highlights model support for the ATA series.

Table 22: Cisco Analog Telephone Adapters

ATA Adapter	10.5(2)x Releases	11.5(x) Releases	12.0(x) Releases	12.5(x) Releases	14(x) Releases
Cisco ATA 190 Analog Telephone Adapter	10.5(2) and later	11.5(1) and later	12.0(1) and later	12.5(1) and later	14 and later

ATA Adapter	10.5(2)x Releases	11.5(x) Releases	12.0(x) Releases	12.5(x) Releases	14(x) Releases
Cisco ATA 191 Analog Telephone Adapter	10.5(2)SU7 and later	11.5(1)SU4 and later	12.0(1)SU2 and later	12.5(1) and later	14 and later

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 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 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.

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 and 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 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 Unified Communications Manager. Ensure 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 (DNA), installed, as a service feature on 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.

Blue Screen Appears for Unified CM Refresh Upgrades

An issue exists with refresh upgrades of Unified Communications Manager to specific destination releases. After the timezone data populates, you may see a blue transition screen appear for 30 minutes or more.

If you see this blue screen, DO NOT stop the upgrade, or a kernel panic occurs. The upgrade will continue to run even while the blue screen displays. The blue screen will clear itself after approximately 30 minutes

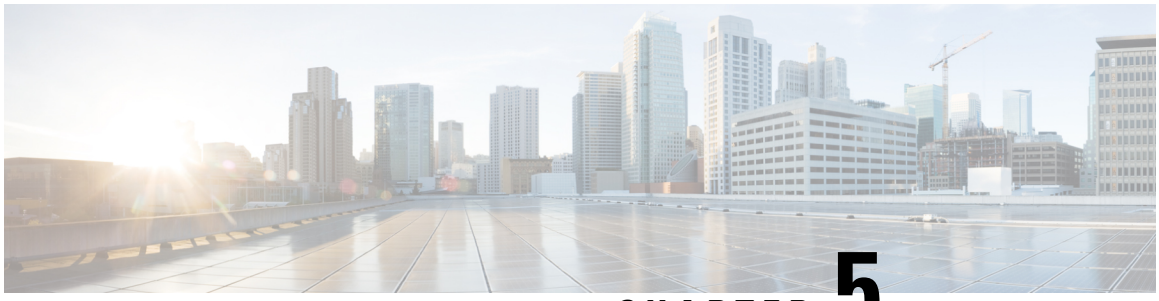
Affected 'To' Versions

This issue affects refresh upgrades of Unified Communications Manager where the destination version falls within the range in the below table. This range includes SU and ES versions that lay within the range. This issue does not occur for upgrades to older or newer versions that do not fall within the range, or for upgrades of the IM and Presence Service.

Table 23: Affected 'To' Versions for Blue Screen Refresh Upgrade Issue

Release Category	Affected Upgrade Destination Range
10.5(x)	10.5.2.21170-1—10.5.2.22188-1 (includes 10.5(2)SU9)
11.5(x)	11.5.1.16099—11.5.1.17118-1 (includes 11.5(1)SU6)
12.0(x)	12.0.1.23036-1 — 12.0.1.24053-1 (includes 12.0(1)SU3)
12.5(x)	12.5.1.11001-1 — 12.5.1.12018-1 (includes 12.5(1)SU1)

For additional details, see CSCvs28202.



CHAPTER 5

Documentation Update for Defects

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

CSCvg70867 Documentation Defect Update

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

CSCvd71818 Documentation Defect Update

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

Reason Code	Description
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)
32	TCPclosedPowerSavePlus - The device closed the TCP connection in order to enter Power Save Plus mode

Reason Code	Description
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
206	DeviceUnregOnSwitchingToDeskphone - The device was unregistered because the client requested to switch from softphone to deskphone control

Reason Code	Description
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

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

Reason Code	Description
27	Power Save Plus
30	Phone Wipe (wipe from CUCM)
31	Phone Lock (lock from CUCM)
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

Reason Code	Description
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
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 24: 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 25: 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 the received offer and preserve it while processing. Select **Off** to enable Unified Communications Manager to ignore the preference of audio codecs in the received offer and apply the locally configured Audio Codec Preference List. The default will select the service parameter configuration. **Note** If this is enabled in both incoming and outgoing trunks then the same codec preference list should be associated with both trunks else it might result in a different codec being negotiated towards both sides leading to audio issues.

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	Cisco 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. 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 Communications Managers 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 IM and Presence Services 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 Cisco 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 Cisco Unified IP Phones 7941/61/70/71/11 when they are in SRST mode only.
Enable VAD	Enables Voice Activation Detection (VAD). When VAD is enabled, media is not transmitted until the voice is detected.

Field	Description
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 Cisco 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 +.
Caller Name	Allows you to enter a caller name to override the caller name that is received from the originating SIP Device.

Field	Description
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 configured on the SIP trunk. After the Unified Communications Manager accepts the call, it uses the configuration for this setting to determine whether the call should get rerouted to another trunk. You can select any of the following method that Unified Communications Manager uses to identify the SIP trunk where the call is rerouted: • Never—If the SIP trunk matches the IP address of the originating device, choose this option, which equals the default setting. The Unified Communications Manager identifies the trunk by using the source IP address of the incoming packet and the signaling port number, do 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. The Unified Communications Manager analyzes 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 number. 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, the Unified Communications Manager analyzes the Call-Info header, search for the parameter purpose=x-cisco-origIP, and uses the IP address or domain name specified in the header to reroute the call to the SIP trunk that uses the IP address and port. The listening port on the inbound trunk and the trunk targeted by the x-cisco-origIP value need to match for the targeted trunk to be used in the call . 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. **Note** You cannot set these parameters as they are not supported in Unified Communications Manager for secure calls. This setting does not work for SIP trunks that are connected to a IM and Presence Service 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, 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. The OPTIONS ping interval value for In-service and Partially In-service ranges from 5 to 600 seconds. The default value is 60 seconds. A SIP trunk is set to In-service when it receives a success response from the peer. If the peer fails to respond due to some errors, then the status is set to Out-of-service. The SIP trunk does not know the peer status until the next time OPTIONS ping is sent. If the SIP trunk sends any message between the ping interval and if the peer destination is Out-of service because of any error, the message results in failure. You can change the ping timer to a smaller value if required. 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.