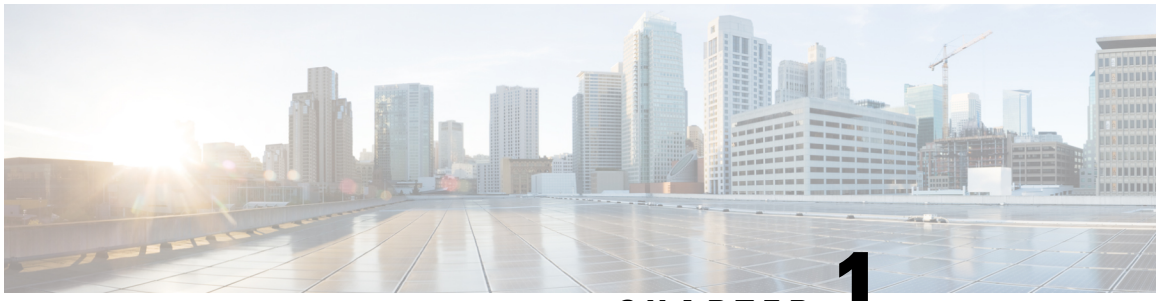
Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 11.5(1)SU8

First Published: 2020-05-21

Last Modified: 2020-06-29

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

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.

Supported Versions

The following table shows supported versions for Release 11.5(1)SU8:

Supported Versions for Release 11.5(1)SU8
Unified Communications Manager 11.5.1.18900-97
IM and Presence Service 11.5.1.18900-15

Release Mismatches

These releases offer two main deployment options for the IM and Presence Service:

- Standard Deployments (Decentralized)—Both Unified Communications Manager and the IM and Presence Service must be running the same release for the deployment to be supported. A mismatch isn't supported. For example, if Unified Communications Manager is running an 11.5(1)SU8 version, the IM and Presence Service must also be running a supported 11.5(1)SU8 version.
- Centralized Deployments of IM and Presence Service—If you have the Centralized Deployment configured on the IM and Presence Service, your IM and Presence Service deployment is running in a different cluster than the Unified Communications Manager telephony deployment. With this option, the IM and

Presence Service deployment can run a different release than the telephony deployment. However, within the IM and Presence central cluster, the Unified Communications Manager publisher node that is located within the IM and Presence central cluster must be running the same release as the IM and Presence Service. This publisher node instance of Unified Communications Manager is for database and user provisioning primarily and doesn't handle telephony.

For example, if the IM and Presence Service central cluster is running Release 11.5(1)SU8, the Unified Communications Manager publisher node within the central cluster must also be running an 11.5(1)SU8 version. However, the telephony deployment can run a different release, such as 11.5(1)SU7.

Documentation Guide

Documentation Guide

For a complete listing of the documents that are available for Release 11.5(1)SU8, see the Documentation Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 11.5(1).

Summary of New and Updated Documents for 11.5(1)SU8

In addition to these Release Notes, the following documents were updated or newly published specifically for Release 11.5(1)SU8:

Document	Description
SU Readme Files	The SU Readme files contain information on the updates and resolved caveats that are a part of Release 11.5(1)SU8. • ReadMe for Cisco Unified Communications Manager Release 11.5(1)SU8 • Read Me for Cisco Unified IM and Presence, Release 11.5(1)SU8
Compatibility Matrix	The 11.5(1)SU5 Compatibility Matrix for 11.5(1)SU5 is updated and retitled to include additional information for 11.5(1)SU8.
Feature Configuration Guide	An 11.5(1)SU8 version of the Feature Configuration Guide is added. This version includes information on how to enable Headset-based Extension Mobility feature and perform Native Phone Migration using IVR and Phone Services.
Command Line Interface Reference Guide	This version provides information about all the commands supported on the IM and Presence Service, Cisco Unified Communications, and Cisco Unity Connection.
Cisco Unified Real-Time Monitoring Tool Administration Guide	This new version also includes updates around PRT reports due to the Cisco Headset Serviceability feature.
Bulk Administration Guide for Cisco Unified Communications Manager	This version provides details on the characters allowed in the files that are uploaded to the Unified Communications Manager server.

Cisco Prime License Manager

Cisco Unified Communications Manager Release 11.5(1)SU3, SU4, SU5, SU6, SU7, and SU8 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.

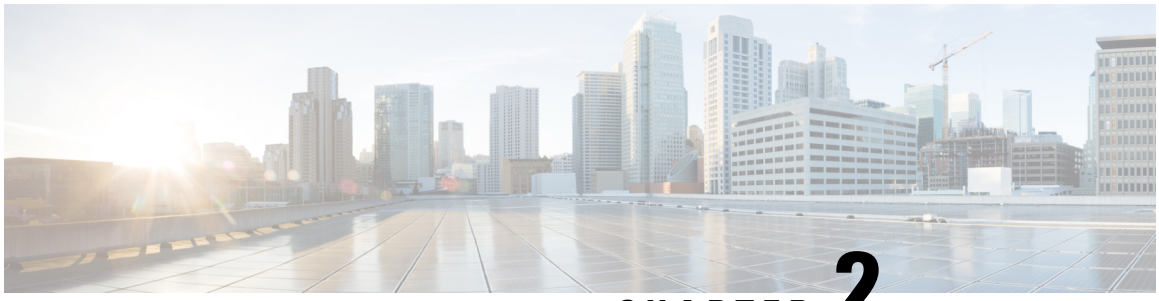
Note With co-resident Prime License Manager deployments, Unified Communications Manager and Cisco Prime License Manager are compatible automatically.

Caveats for 11.5(1)SU8

Caveats for 11.5(1)SU8

For a list of Open Caveats and Resolved Caveats, see the respective Readme files:

- ReadMe for Cisco Unified Communications Manager Release 11.5(1)SU8
- Read Me for Cisco Unified IM and Presence, Release 11.5(1)SU8



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.

Supported Upgrade and Migration Paths

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

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

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

Deployments on Cisco Media Convergence Servers Hardware

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

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

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

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

Table 1: 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 2: 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 3: 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)	11.5(x)	PCD Migration PCD Upgrade (Direct Standard) Cisco Unified OS Admin (Direct Standard)
11.0(1)	11.5(x)	Cisco Unified OS Admin (Direct Standard) PCD Migration PCD Upgrade (Direct Standard)
11.5(x)	11.5(y)	Cisco Unified OS Admin (Direct Standard) PCD Migration PCD Upgrade (Direct Standard)

Table 4: 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)

From	To	Supported Method
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)

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 5: 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

From	To	Upgrade Type
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 6: 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 7: 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, and SU8 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

Deprecated Endpoints

The following phone models are deprecated and are not supported by Cisco Unified Communications Manager Release 11.5(x). If you are using any of these phone models and you upgrade to release 11.5(x), you will be unable to use the phone after the upgrade. After you switch over to the new release, registration on the phone will be blocked.

- 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

Upgrades that Involve Deprecated Phones

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

1. Confirm whether the phones in your network will be supported in Release 11.5.
2. Identify any non-supported phones.
3. For any non-supported phones, power down the phone and disconnect the phone from the network.
4. Provision a supported phone for the phone user. You can use the Migration FX tool to migrate from older model to newer model phones. For details, go to: http://refreshcollab.cisco.com/webportal/46/CUCM%20Readiness%20Assessment#endpoint_refresh_tool.
5. Once all the phones in your network are supported by Release 11.5, upgrade your system.

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

Licensing

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

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

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

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

Standard Deployments of IM and Presence

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

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

Centralized Deployment Exception

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

Upgrading with FIPS Mode Enabled

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

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

You can either:

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

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

Upgrades with Mixed Mode Enabled Require an Encryption License

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

If you upgrade from an earlier release with mixed-mode enabled, but you do not have an encryption license installed, a warning message on the encryption license requirement displays on the user interface immediately 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.

Ordering and Installing License Files

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

Table 8: 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 9:

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**

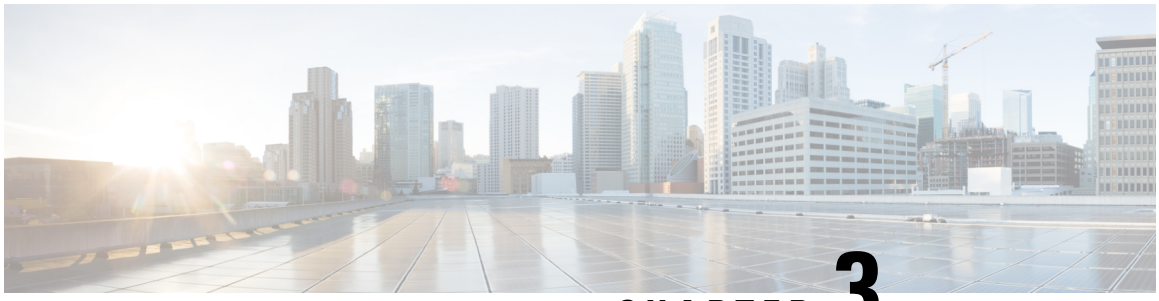
b. Uncheck the following check boxes:

- **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 document.



CHAPTER 3

New and Changed Features

Calendar Integration with Office 365 Support for OAuth 2.0 authentication

The IM and Presence Service's Calendar Integration with Office 365 feature is enhanced to support the usage of OAuth tokens for authenticating to the Office 365 server. This enhancement allows a more streamlined and secured authentication process than the regular password-based authentication.

When you configure Calendar Integration with an Office 365 server, the IM and Presence Service lets you choose from two authentication options:

- **Basic**—password-based logins
- **OAuth**—authentication with OAuth tokens

Note Basic authentication method will be supported as long as Microsoft supports it. When Microsoft deprecates, it will be deprecated from IM and Presence Service.

If you choose OAuth, you must configure the following fields, each of which are added to the Presence Gateway Configuration window for this release. These fields are included for OAuth logins only:

- Application (client) ID
- Directory (tenant) ID
- Client Secret

For more information on how to configure the IM and Presence Service for Calendar Integration with an Office 365 server, see the Microsoft Outlook Calendar Integration for the IM and Presence Service.

Cisco Headset and Finesse Integration for Contact Center

Cisco Headset and Finesse Integration improves productivity of contact center agents by giving them the ability to change the agent Ready/Not Ready status right from their Cisco headset. When this feature is turned on, the headset Mute button acts as a Ready/Not Ready button when the call agent is idle. This lets the agent control whether they are ready to take another call without having to go into the Finesse desktop. All agent status is synced between the headset and Cisco Finesse so that the current status is known by both. During calls, the headset Mute button retains existing functionality as a Mute/Unmute button.

This feature is available as a preview feature with Cisco Unified Communications Manager, Release 11.5(1)SU8 and is targeted to Contact Center deployments. You can deploy the feature for internal testing and development, but we do not recommend that you deploy the feature in a production environment. All support requests to Cisco TAC are treated as severity-level 4. Full support is expected to be added in a future release.

To use the feature, you must turn the feature on via an enterprise parameter. The configuration menus become active only after the enterprise parameter is enabled. For complete information on how to deploy and configure this feature, see the white paper *Cisco Headset and Finesse Integration for Contact Center* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cucm/whitePaper/CUCM_Headsets_for_ContactCenter_WP.pdf.

Emergency Call Routing Regulations

The US Federal Communications Commission (FCC) has signed the Call Routing Regulations requesting Multi-Line Telephone Systems (MLTS) Systems to provision or enforce direct 911 dial (without any prefix dialing). The Unified Communications Manager is responsible for routing all emergency calls in agreement with the FCC rules.

Unified CM installed or upgraded fully or partly in regions where the FCC rules are applicable, detects the presence of a direct dial 911 Route Pattern and disables further notifications to the administrator.

If the 911 pattern doesn't exist, Unified CM sends an alert notification to an administrator to create the 911 Route pattern.

An administrator must consult their legal counselor on the applicability of the law and acknowledge along with performing necessary configurations or disable further notifications if not applicable. For more information on acknowledging and acceptance of law, see the chapter "The US Federal Communications Commission (FCC) Emergency Call Routing Regulations" in the Feature Configuration Guide for Cisco Unified Communications Manager.

Extension Mobility Login Simplification using Headset

The Headset-based Extension Mobility is a new feature introduced to create an association (user's identity) between headsets and end users. An administrator and the end users can associate headsets from any devices such as self-owned devices, shared spaces, and common area devices. This association helps in authentications and creating customized experience for its users. One such customized experience is to use an associated headset for Extension Mobility login to have a seamless login experience.

For more information, see the "Headset Service" chapter in Feature Configuration Guide for Cisco Unified Communications Manager.

User Interface Updates

To support this feature, the following parameters and fields are added:

1. In the **System** > **Enterprise Parameters Configuration** page, a new parameter **Headset Association** is added to enable end users to associate headset using the **Headset Association** menu option on the device screen. The following options are available in the new parameter:
   - Prompt user to initiate Headset Association from all devices
   - Prompt user to initiate Headset association only from Extension Mobility-enabled devices
   - Do not prompt user to initiate Headset association from all devices
2. In the **System** > **Service Parameters** page, the following two new parameters are added in **Clusterwide Parameters (Parameters that apply to all servers)** section to allow headset for Extension Mobility sign in and sign out and configure maximum duration that the system can wait for user input when the headset is disconnected from the device before automatically logging out the user.
   - Headset-based Extension Mobility
     - Allow headset for Extension Mobility sign in and sign out
     - Do not Allow headset for Extension Mobility sign in and sign out
   - Auto logout timer after headset disconnect (minutes)
3. In the **User Management** > **End User** > **End User Configuration** page, a new field is added under the Associated Headsets section.
   - Headset Serial Number

For more information, see the **User Management Menu** > **About End User Setup** > **End User Settings** section in the *Cisco Unified Administration CM Administration Online Help*.

Native Phone Migration using IVR and Phone Services

The Phone Migration feature is an easy and intuitive Cisco IP Phone migration solution native to Unified Communications Manager. It minimizes the cost and complexity of replacing deprecated or faulty phones. Using this solution, an end user or an administrator can easily migrate all the settings from an old phone to a new phone with a simple user interface. Solution supports the following methods for migration the phones:

- **Using Self-provisioning IVR Service**
- **Using Phone Migration Service**
- **Using Cisco Unified CM Administration Interface**

Following table provides a quick comparison of the various phone migration options:

Table 10: Different Phone Migration Options and Considerations

	Using Self-provisioning IVR Service	Using Phone Migration Service	Using Unified CM Administration Interface
End user or administrator driven phone migration	End user (Self-service)	End user (Self-service)	Administrator
Auto-registration required	Yes	No	No
Migration steps	• Auto register a new phone • Dial self-provisioning IVR number • Follow the voice prompts	• Plug-in new phone to the network • Key in primary extension and PIN (optional)	• Sign in to Cisco Unified CM Administration interface • Choose "Migrate Phone" option in the Phone Configuration page of the old phone • Enter phone type (model & protocol) and MAC address of the new phone
Administrator involvement	Medium	Low	High

For more information, see the "Native Phone Migration using IVR and Phone Services" chapter in Feature Configuration Guide for Cisco Unified Communications Manager.

User Interface Updates

To support this feature, the following sections are added:

- In the **System > Enterprise Parameters Configuration** page, a new section **Phone Migration** is added. The following options are available in the new section:
  - **When Provisioning a Replacement Phone for an End User** drop-down list is added.
  - **Security Profile for Migrated Phone** drop-down list is added.
- In the **User Management > User Settings > User Profile Configuration** page, a new check box is added under the **Self-Provisioning** section.
  - **Allow Provisioning of a phone already assigned to a different End User**
- In the **Find and List Phones Configuration** page, a new drop-down list **Migrated (old phone)** is added.

For detailed information on the new parameters and fields, see the *Cisco Unified Administration CM Administration Online Help*.

Phone Feature Updates

The Phone Configuration Layout for the Cisco IP Phone 8800 Series of phones is updated to allow you to configure support for the following phone features right from the Unified CM Phone Configuration window:

- **Mark Your Calls as Spam**—You can use the Mark spam feature to reduce the number of unwanted phone calls that you receive. With this feature, you designate a phone number as either a potentially fraudulent call or as a telemarketer call.
- **Lower Your Voice**—If you speak in a loud voice, you can set your phone to remind you to speak at an appropriate level by displaying a warning message on the phone.

Note Minimum supported phone version is Release 12.8.1 and above.

You can configure these features in the Product Specific Configuration Layout area of your phone model in the Cisco Unified CM Administration interface or the Phone directly.

For more information, see the Cisco IP Phone 8800 Series Administration Guide for Cisco Unified Communications Manager.

Push Notification Deployment for iOS 13

This release of Cisco Unified Communications Manager and the IM and Presence Service includes updates to Push Notifications in support of Apple's iOS 13 implementation.

Jabber 12.9 release is built using iOS 13 SDK. Under iOS 13, Apple processes Push Notifications for suspended applications differently than it did with iOS 12. Following is a summary of the Apple Push Notification service updates that are introduced with iOS 13:

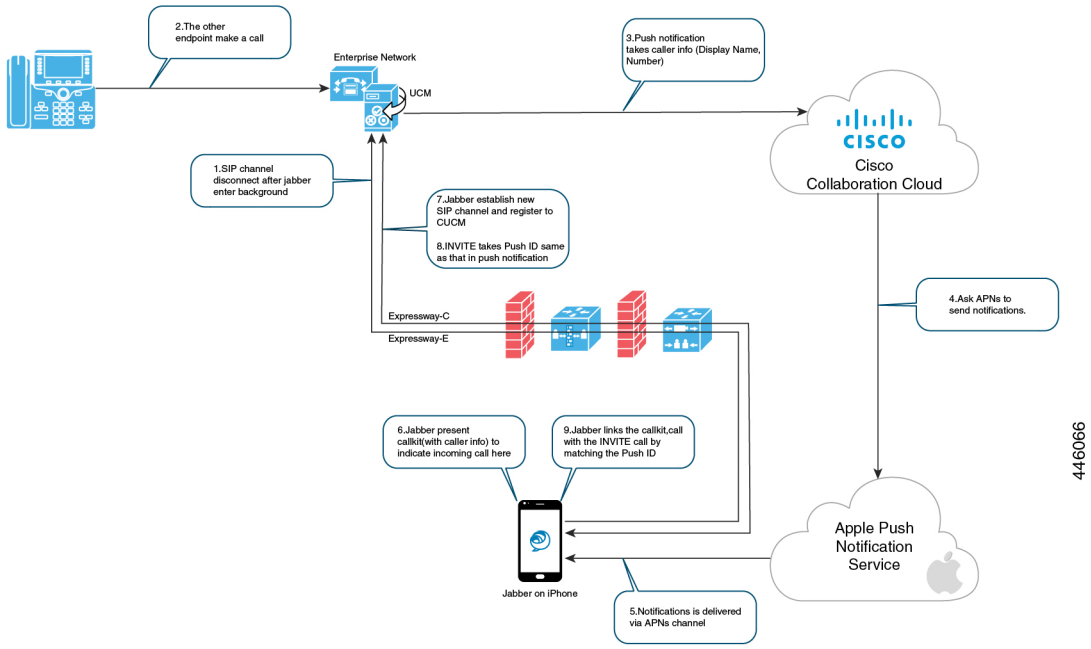
- Push Notifications under iOS 13 are delivered using a "VoIP" channel for calls and a separate "Message" channel for messaging. This is in contrast to iOS 12 where all Push Notifications traffic were delivered using the same channel.
- iOS clients, upon receiving a VoIP push notification, launch CallKit immediately to indicate an incoming call.
- Push Notifications "VoIP" traffic includes caller identity information (Display Name and Number), which the client uses to populate the CallerID field in CallKit.
- Push Notifications of type "VoIP" are considered high priority and are delivered without delay.

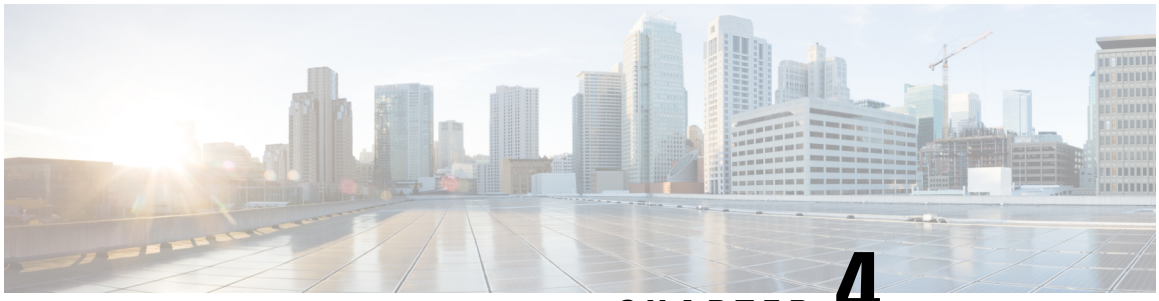
For up-to-date support information related to the Apple Push Notification service under iOS 13, including upgrade requirements, see the Apple Push Notification Service Updates.

For information on how to deploy Push Notifications, see the Push Notifications Deployment for Cisco Jabber on iPhone and iPad with Cisco Unified Communications Manager.

iOS 13 Call Flow

The following diagram illustrates the process for calls that use the Push Notifications 'VoIP' channel under iOS 13.





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 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

This information applies to CSCuz42260.

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).

New Cisco Gateway Support

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

- Cisco VG400 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 Cisco Unified Communications Manager.

Table 11: 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
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
Cisco VG400 Analog Voice Gateway	Not supported	11.5(1)SU7 and later	12.0(1)SU2 and later	12.5(1) 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
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
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

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 12: Cisco Analog Telephone Adapters

ATA Adapter	10.5(2)x Releases	11.5(x) Releases	12.0(x) Releases	12.5(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
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

Tomcat Certificate Regeneration with SAML SSO Deployment

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

IM and Presence Service

Intercluster Peering Not Supported with Cisco Unified Presence 8.6

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

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.

Block Message Delivery Not Supported

The **IM Compliance Configuration** online help for the IM and Presence Service, Release 11.5(1)SU5 contains a message for the **Block message delivery if unable to record in compliance database** check box. However, this option is not available with this release. If you require this option, you must upgrade to a 12.x release.

Miscellaneous

Bandwidth Allocations for 88xx SIP Phones

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

Dialed Number Analyzer does not Support Single Sign-On

Dialed Number Analyzer does not support Single Sign-On

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

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

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

Route Filter and Associated Route Patterns

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

Blue Screen Appears for Unified CM Refresh Upgrades

An issue exists with refresh upgrades of Cisco 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 13: 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.