Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 11.5(1)SU9—SU11

First Published: 2020-12-15

Last Modified: 2023-01-31

CONTENTS

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)SU9, SU10, and SU11

Release	Full Version Number
Release 11.5(1)SU9	• Unified Communications Manager 11.5.1.21900-40 • IM and Presence Service 11.5.1.21900-5
Release 11.5(1)SU10	• Unified Communications Manager 11.5.1.22900-28 • IM and Presence Service 11.5.1.22900-6
Release 11.5(1)SU11	• Unified Communications Manager 11.5.1.23900-30 • IM and Presence Service 11.5.1.23900-3

Documentation Guide

Documentation Guide

For a complete listing of the documents that are available for Release 11.5(1)SU9, SU10, and SU11, 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)SU9, SU10 and SU11

In addition to these Release Notes, the following documents were updated or newly published specifically for Release 11.5(1)SU9, SU10, and SU11:

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)SU9, SU10, and SU11. • ReadMe for Cisco Unified Communications Manager Release 11.5(1)SU9 • Read Me for Cisco Unified IM and Presence, Release 11.5(1)SU9 • ReadMe for Cisco Unified Communications Manager Release 11.5(1)SU10 • Read Me for Cisco Unified IM and Presence, Release 11.5(1)SU10 • ReadMe for Cisco Unified Communications Manager Release 11.5(1)SU11 • Read Me for Cisco Unified IM and Presence, Release 11.5(1)SU11
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)SU9, SU10, and SU11.
Cisco Unified Real-Time Monitoring Tool Administration Guide	This new version includes support for Windows 2019 for the Cisco Unified Real-Time Monitoring Tool.
Feature Configuration Guide	This version includes updates to the Native Phone Migration using IVR and Phone Services feature. In addition, updates are added to the 'Manager Assistant' chapter to include the information that Oracle Java Runtime Environment (JRE) is no longer included in the Cisco Unified Communications Manager Assistant plug-in.
Security Guide	The book includes enhanced information on a subject like Cipher negotiations that help you make security decisions for your deployment.
Upgrade and Migration Guide	Includes updates for Release 11.5(1)SU10 that includes Daylight Savings Time and Spectre/Meltdown vulnerabilities during upgrades.

Document	Description
Administration Guide	Use this guide to complete administrative tasks on a configured Cisco Unified Communications Manager system.
SAML SSO Deployment Guide	Use this guide to learn key concepts, terminology, and high-level information that you need to configure and enable the SAML-based SSO solution across a defined set of Cisco collaboration applications.

Cisco Prime License Manager

Cisco Unified Communications Manager Release 11.5(1)SU3, SU4, SU5, SU6, SU7, SU8, SU9, SU10, and SU11 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)SU9, SU10 and SU11

Caveats for 11.5(1)SU9

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

- ReadMe for Cisco Unified Communications Manager Release 11.5(1)SU9
- Read Me for Cisco Unified IM and Presence, Release 11.5(1)SU9

Caveats for 11.5(1)SU10

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

- ReadMe for Cisco Unified Communications Manager Release 11.5(1)SU10
- Read Me for Cisco Unified IM and Presence, Release 11.5(1)SU10

Caveats for 11.5(1)SU11

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

- ReadMe for Cisco Unified Communications Manager Release 11.5(1)SU11

- Read Me for Cisco Unified IM and Presence, Release 11.5(1)SU11

Upgrades

Upgrade Procedures

Note If your pre-upgrade version is Release 11.5(1)SU9 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).

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 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)

From	To	Supported Method
9.1(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Refresh) Cisco Unified OS Admin (Direct Refresh)
10.0(x)	11.5(x)	PCD Migration PCD Upgrade (Direct Standard)
10.5(x)	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)
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)

From	To	Supported Method
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 5: 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 6: 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 7: 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 8: 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, SU9., SU10, and SU11 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 Users Should be Logged Out During Upgrade

When upgrading the IM and Presence Service, it's best to ensure that all Cisco Jabber users are logged out during the upgrade. The more Cisco Jabber user activity you have, the greater the likelihood that you will receive an error that requires administrator intervention such as a Presence status sync error.

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)SU2. 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)SU2.

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 9: 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 10:

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

Emergency Calling for National Suicide Prevention Lifeline

Unified Communications Manager supports dialing '988' calls, that are 3-digit dialing codes that will be routed to the National Suicide Prevention Lifeline centers. All telecommunication carriers and interconnected voice over Internet Protocol (VoIP) service providers will offer this service to connect with suicide prevention and mental health crisis personnel. This is in support of the FCC mandate of supporting a 3-digit dial code for Suicide Prevention Hotline that comes into effect from July 22, 2022.

For more information, see: https://www.fcc.gov/suicide-prevention-hotline.

JTAPI Plugin Support

Cisco JTAPI plug-in follows the installer less approach from Release 11.5(1)SU9 onwards. Click the corresponding Cisco JTAPI Client for Linux (32 and 64 bit) or Cisco JTAPI Client for Windows (32 and 64 bit) link to download zip files (CiscoJTAPIWindows.zip or CiscoJTAPILinux.zip) available in the Cisco Unified CM Administration interface.

For more information, see the "Installation Procedures" section in the Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager, Release 11.5(1).

Oracle JRE Removal from Manager Assistant

The Oracle Java Runtime Environment (JRE) is no longer included in the Cisco Unified Communications Manager Assistant plug-in.

Before you upgrade the Cisco Unified Communications Manager Assistant client to a newer version, perform the following:

- Uninstall the Cisco Unified Communications Manager Assistant client that is currently installed on your machine.

- Install JRE on 32-bit or 64-bit Windows platform.

For more information, see the Feature Configuration Guide for Cisco Unified Communications Manager.

UDS Performance Improvement

The UDS Bulk Search by Email enables Cisco Jabber to send requests in batches using the email attribute to prevent high CPU usage by UDS and Cisco Tomcat services.

Windows 2019 Support for RTMT

You can install Cisco Unified Real-Time Monitoring Tool on a computer that is running on Windows 2019 operating system to monitor or troubleshoot Unified Communications Manager.

Improved IM and Presence Stream Features/Services Advertisement via Expressway

IM and Presence Service now has an enhanced mechanism of advertising XMPP stream features/services (mdm:1, push:3, and so on) to the clients connecting over Cisco Expressway's Mobile and Remote Access (MRA).

The new design supports deployments consisting of IM and Presence clusters with mixed versions. For example, some IM and Presence clusters run 11.5(1) SU7 and some clusters are upgraded to 11.5(1) SU9. This ensures that the client always gets the correct list of supported or enabled stream features from the version of the IM and Presence server that the end user is assigned to.

For this mechanism to work, the minimal deployment requirement is to have Cisco Expressway running version not older than X12.7, and to have at least one IM and Presence cluster in the intercluster mesh running version 11.5(1) SU9 or above.

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).

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 (for example, 11.5(x) and 12.5(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 11: Cisco Gateways with Initial Release By Release Category

Gateway Model	11.5(x) Releases	12.5(x) Releases	14(x) Releases
Cisco VG 202, 202 XM, 204, 204 XM, 310, 320, 350 Analog Voice Gateway	11.5(1) and later	12.5(1) and later	14 and later
Cisco VG400 Analog Voice Gateway	11.5(1)SU7 and later	12.5(1) and later	14 and later
Cisco VG420 Analog Voice Gateway	Not supported	12.5(1)SU4 and later	14SU1 and later
Cisco VG450 Analog Voice Gateway	11.5(1)SU6 and later	12.5(1) and later	14 and later
Cisco 4321, 4331 4351, 4431, 4451 Integrated Services Router	11.5(1) and later	12.5(1) and later	14 and later
Cisco 4461 Integrated Services Router	11.5(1)SU6 and later	12.5(1) and later	14 and later
Cisco Catalyst 8300 Series Edge Platforms	—	12.5(1)SU4 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 12: Cisco Analog Telephone Adapters

ATA Adapter	11.5(x) Releases	12.5(x) Releases	14(x) Releases
Cisco ATA 190 Analog Telephone Adapter	11.5(1) and later	12.5(1) and later	14 and later
Cisco ATA 191 Analog Telephone Adapter	11.5(1)SU4 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.

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 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.