Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 11.5(1)SU5 and SU6

First Published: 2018-06-29

Last Modified: 2020-03-20

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1 **About this Release** 1

Revision History 1

Introduction 1

Supported Versions 2

Documentation for this Release 3

Cisco Prime License Manager 4

Caveats 4

CHAPTER 2 **Upgrades** 7

Upgrade Procedures 7

Supported Upgrade and Migration Paths 7

Deployments on Cisco Media Convergence Servers Hardware 8

Deployments on Virtual Machines 8

COP Files Required for Upgrades to Release 11.5 10

Requirements and Limitations 11

Upgrade Requirements with Standalone Prime License Manager 12

Cisco Jabber During Upgrade 12

Deprecated Phone Models 12

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

Rolling Back to Previous Versions 13

Upgrading with FIPS Mode Enabled 13

Upgrades with Mixed Mode Enabled Require an Encryption License 14

Database Migration Required for Upgrades with Microsoft SQL Server 15

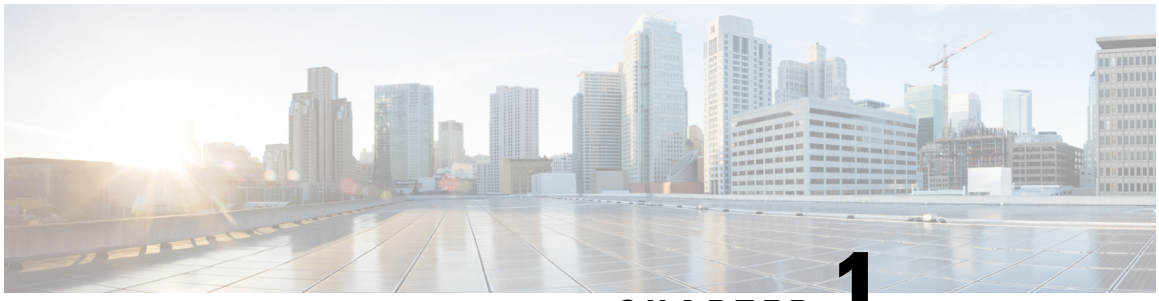
Upgrades from 11.5(1)SU2 with Push Notifications Enabled 17

CHAPTER 3 **New and Changed Features** 19

AES 80-Bit Authentication Support 19
Call Recording for SIP TLS Authenticated calls 19
Encrypted IM Compliance Database 20
Immediate Divert to Voicemail for WebEx Hybrid Services 23
Persistent Chat Support on Jabber Mobile 23
Push Notifications Updates 24
Search Conference Rooms via UDS Proxy for LDAP 24

CHAPTER 4 **Important Notes** 27

Features and Services 27
Media Sense does not record the Consult Call with Selective Recording 27
OVA Requirements and User Capacities 27
SDL Listening Port Update Requires CTIManager Restart on all Nodes 28
Interoperability 28
AXL Requests to Unified CM Nodes 28
Cisco Unified Attendant Console Support 28
IM and Presence Service Interoperability with Expressway-C 28
New Cisco Gateway Support 28
Tomcat Certificate Regeneration with SAML SSO Deployment 30
IM and Presence Service 30
Intercluster Peering Not Supported with Cisco Unified Presence 8.6 30
IM and Presence Server Pings to Jabber Are Not Configurable 30
Persistent Chat Character Limit with Microsoft SQL Server 30
Rebooting IM and Presence Subscriber Nodes 30
Block Message Delivery Not Supported 30
Miscellaneous 31
Bandwidth Allocations for 88xx SIP Phones 31
Dialed Number Analyzer does not Support Single Sign-On 31
Route Filter and Associated Route Patterns 31
Blue Screen Appears for Unified CM Refresh Upgrades 31



CHAPTER 1

About this Release

- Revision History, on page 1
- Introduction, on page 1
- Supported Versions, on page 2
- Documentation for this Release, on page 3
- Cisco Prime License Manager, on page 4
- Caveats, on page 4

Revision History

Date	Description of Changes
June 07, 2019	Added link to Caveats in the Readme file.
June 29, 2018	Initial publish
July 03, 2018	Updated build numbers for IM and Presence Service. Added links to published documents.
April 08, 2019	Updated OVA requirements around Centralized Deployment.
January 13, 2020	Updated Documentation for this Release to more communicate the documentation updates for this release, along with where to get a complete listing of applicable documents for this release (Documentation Guide).
January 30, 2020	Added Important Note on gateway support.
February 12, 2020	Added important note on blue screen appearing during certain refresh upgrades.

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 table shows supported versions for Release 11.5(1)SU5 and SU6.

Supported Versions for Release 11.5(1)SU5	Supported Versions for Release 11.5(1)SU6
Cisco Unified Communications Manager 11.5.1.15900-18	Cisco Unified Communications Manager 11.5.1.16900-16
IM and Presence Service 11.5.1.1.15900-33	IM and Presence Service 11.5.1.16910-12

Release Mismatches

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

- Standard Deployments (Decentralized)—Both Cisco Unified Communications Manager and the IM and Presence Service must be running the same release for the deployment to be supported. A mismatch is not supported. For example, if Cisco Unified Communications Manager is running an 11.5(1)SU5 version, the IM and Presence Service must also be running a supported 11.5(1)SU5 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 Cisco 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 Cisco 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 Cisco Unified Communications Manager is for database and user provisioning primarily and does not handle telephony.

For example, if the IM and Presence Service central cluster is running Release 11.5(1)SU5, the Unified Communications Manager publisher node within the central cluster must also be running an 11.5(1)SU5 version. However, the telephony deployment can run a different release, such as 11.5(1)SU6.

Documentation for this Release

Documentation Guide

For a complete listing of the documentation that is available for Releases 11.5(1)SU5 and SU6, see the *Documentation Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 11.5(1* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/docguide/11_5_1/cucm_b_documentation-guide-cucm-imp-1151.html.

Summary of New and Updated Documents

The following table summarizes the documents that were newly published specifically for Release 11.5(1)SU5 or SU6:

Document	Description
SU Readme Files	Refer to either of the Readme Files for information on updates and bug fixes that are included in your release **Readme Files for 11.5(1)SU5** • ReadMe for Cisco Unified Communications Manager Release 11.5(1)SU5 • Read Me for Cisco Unified IM and Presence, Release 11.5(1) SU5a **Readme Files for 11.5(1)SU6** • Readme File for Cisco Unified Communications Manager 11.5(1)SU6 • Readme File for Cisco Unified CM IM and Presence Service 11.5(1)SU6
Compatibility Matrix	A new version of the Compatibility Matrix exists for 11.5(1)SU5 and later. This guide is enhanced to include additonal compatibility items such as operating system support, supported ciphers, and additional integrations.

Document	Description
Configuration and Administration for the IM and Presence Service	A new version of this guide exists for 11.5(1)SU5 and later. This document has been completely rewritten and restructured from previous versions. This enhanced version features the following documentation improvements: • Extensive configuration task flows to provide a more complete and simpler system configuration process. This new flow also reduces the need to refer to Cisco Unified Communications Manager books for most IM and Presence configurations. • Smoother chapter flow that matches the configuration process and which provides better navigation. • A new Planning chapter that outlines some basic things to decide on before you deploy your system.
Instant Messaging Compliance for the IM and Presence Service	A new version of this document exists for 11.5(1)SU5 and later. The Message Archiver configuration process has been restructured, and updated. Among the updates are details for how to deploy an encrypted IM compliance database.
Real_Time Monitoring Administration Guide—11.5(1)SU6	A new version of this guide exists for 11.5(1)SU6, due to updates around JRE installation.

Cisco Prime License Manager

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

Caveats for 11.5(1)SU5

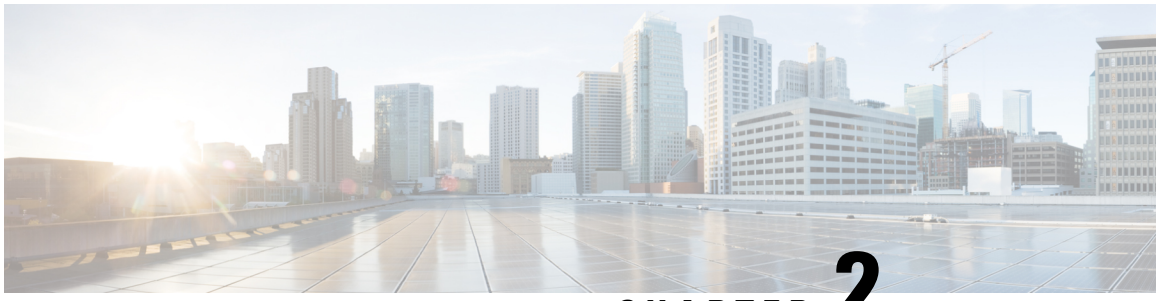
For a list of open and resolved caveats, refer to the Readme files:

- Readme File for Cisco Unified Communications Manager, Release 11.5(1)SU5
- Readme File for Cisco Unified CM IM and Presence Service, Release 11.5(1)SU5

Caveats for 11.5(1)SU6

For a list of open and resolved caveats, refer to the Readme file:

- Readme File for Cisco Unified Communications Manager, Release 11.5(1)SU6
- Readme File for Cisco Unified CM IM and Presence Service, Release 11.5(1)SU6



CHAPTER 2

Upgrades

- Upgrade Procedures, on page 7
- Supported Upgrade and Migration Paths, on page 7
- Requirements and Limitations, on page 11

Upgrade Procedures

Note If your pre-upgrade version is Release 11.5(1)SU7 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)

From	To	Supported Method
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)

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, and SU7 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

Upgrades that Involve Deprecated Phones

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

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

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

Licensing

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

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

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

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

Rolling Back to Previous Versions

Standard Deployments of IM and Presence

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

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

Centralized Deployment Exception

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

Upgrading with FIPS Mode Enabled

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

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

You can either:

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

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

Upgrades with Mixed Mode Enabled Require an Encryption License

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

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

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

Ordering and Installing License Files

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

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

Database Migration Required for Upgrades with Microsoft SQL Server

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

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

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

Before You Begin

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

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

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

Upgrades from 11.5(1)SU2 with Push Notifications Enabled

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

After you upgrade your system, do the following:

Procedure

Step 1 Disable Push Notifications

Follow these steps:

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

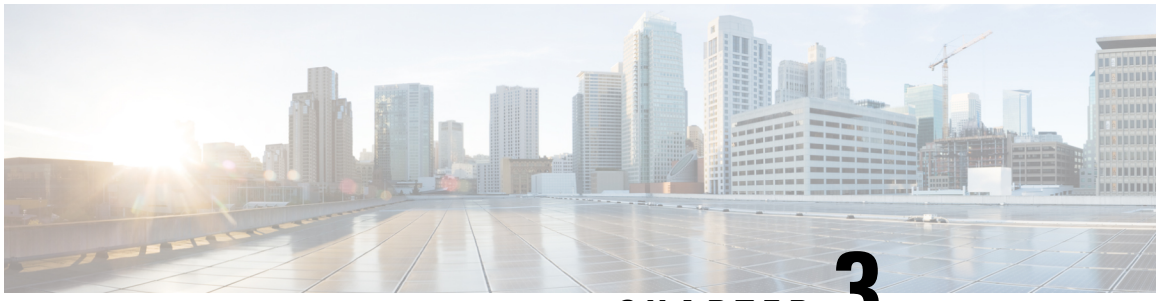
b. Uncheck the following check boxes:

- **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 at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/pushNotifications/11_5_1_su2/cucm_b_push-notification-deployment-iPhone-iPad.html.



CHAPTER 3

New and Changed Features

The following new and changed feature was introduced for Release 11.5(1)SU7:

- AES 80-Bit Authentication Support, on page 19
- Call Recording for SIP TLS Authenticated calls, on page 19
- Encrypted IM Compliance Database, on page 20
- Immediate Divert to Voicemail for WebEx Hybrid Services, on page 23
- Persistent Chat Support on Jabber Mobile, on page 23
- Push Notifications Updates, on page 24
- Search Conference Rooms via UDS Proxy for LDAP, on page 24

AES 80-Bit Authentication Support

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

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

Call Recording for SIP TLS Authenticated calls

Prior to 11.5(1)SU5 version, the phones that are authenticated (phone with security profile having **Device Security Mode** as **Authenticated**) were not allowed to make use of the **Call Recording** feature. Whereas, non–secured phones or secured/ encrypted phones could use call recording feature with non-secured or secured recorders, respectively. With this release 11.5(1)SU5, Cisco Unified Communications Manager allows call recording for authenticated phones while using non secure recorder. In case of secure recorder, recording is allowed only if the recorder supports Secure Real-Time Transport protocol (SRTP) fallback.

To record a call for authenticated phones, On the Cisco Unified Communications Manager Service Parameter page, set the **Authenticated Phone Recording field** to **Allow Recording**. The default value is **Do Not Allow Recording**.

Cisco Unified Communications Manager JTAPI/TAPI interface has been enhanced to allow recording in Authenticated phone, based on the value of the new service parameter - **Authenticated Phone Recording**. Now, the expectation is that the call recording can be done by Authenticated phones also. The value of newly added service parameter can be set as as follows:

- **Allow Recording** – Authenticated phones can record the calls..
- **Do Not Allow Recording** – Authenticated phones cannot record the calls. This will be the default value for the service parameter. The behavior would be the same as that of the current behavior.

  This feature is backward compatible. JTAPI/TAPI will support the current API's.

Encrypted IM Compliance Database

This release of the IM and Presence Service supports an encrypted compliance database for the Message Archiver feature. When this feature is deployed, all instant messages are encrypted before they get sent to the compliance database. Anyone looking at the data within the compliance database is unable to read the archived messages without an encryption key.

This feature provides greater security for your IM and Presence deployment by allowing your system to comply with compliance regulations, while restricting read access for potentially confidential IM exchanges to authorized personnel. For example, let's say that your company uses instant messaging to communicate with customers, and your company does business in a regulated industry that requires message archiving. By restricting access to the encryption key, you can archive all instant messages, provide employees such as a database administrator with the database access that they need to keep the system running, while still limiting read access to archived IM exchanges to only those employees with a genuine business need.

This feature is supported only if you have Microsoft SQL Server deployed as the external compliance database.

Intercluster Networks

For intercluster networks, you can enable encryption for the intercluster network from a single cluster, which then becomes the master cluster for the network. The master cluster syncs its encryption key and encryption settings to the remote clusters, which become the slave clusters in the intercluster network. Encryption is configured automatically for remote clusters, provided the Message Archiver feature is configured in the remote cluster, with a Microsoft SQL Server compliance database.

Encryption Standards

To ensure that archived data is not compromised, this feature uses three keys: a symmetric encryption key, along with an assymetric public-private key pair.

- Encryption key—This 256-bit symmetric key is generated and stored internally by the IM and Presence Service, which uses this key to encrypt IM compliance data before archiving the data in the compliance database. For intercluster networks, the master cluster syncs its encryption key to the remote slave clusters so that the entire intercluster network is using the same encryption key, which is controlled from the master cluster.

  You must download this key from the IM and Presence Service and use it with your data viewer to be able to decrypt archived IMs. When you download this key, the key is encrypted with the public key from the public-private key pair. You can later decrypt the encryption key with the private key.

- Public-Private key pair—You must generate this assymetric key pair in an approved key generation tool (for example, OpenSSL) and use it to encrypt the key in the IM and Presence Service and then decrypt

the key with your data viewing tool. The public-private key pair secures the encryption key while in transit from the IM and Presence Service to your data viewing tool (for example, Splunk).

The encryption password is hashed with SHA2 and then encrypted with AES 256. Instant Messages are encrypted with the AES 256 algorithm

Process Flow for Encryption

The following table highlights the process flow for enabling encryption and for viewing encrypted data from the database. The flow highlights each step, and the interface on which each step is completed.

Table 10: Encryption Process Flow

	IM and Presence Service Master Cluster	Key Generation Tool (e.g., OpenSSL)	Data Viewing Tool
Step 1	The administrator configures encryption for the intercluster network. The master cluster syncs encryption settings across the intercluster network. Archived data is now encrypted.	—	—
Step 2	—	The administrator generates a public-private key pair for securing the encryption key.	—
Step 3	The administrator downloads the encryption key from the IM and Presence Service. During the download, the public key encrypts the encryption key.	—	—
Step 4	—	—	The administrator uses the private key to decrypt the encryption key.
Step 5	—	—	The encryption key decrypts compliance data. Authorized personnel can view archived compliance data.

Minimum Requirements

The following requirements apply for this feature

Table 11: Minimum Requirements for Encrypted IM Compliance Database

System	Requirements for this Feature
IM and Presence Service	• For 11.x releases, the minimum release for this feature is 11.5(1)SU5. • For 12.x releases, the minimum release will be 12.5(1). • This feature is not supported with 12.0(1) or 12.0(1)SU1. If you have this feature deployed in 11.5(1)SU5 and you upgrade to 12.0(1) or 12.0(1)SU1, you will lose this feature.
External Database	• You must have Microsoft SQL Server deployed as your compliance database on all cluster nodes to support this feature.

Configuration

For details on how to configure an encrypted database for the Message Archiver, refer to the "Message Archiver Configuration" chapter of the *Instant Messaging Compliance Guide for the IM and Presence Service.*

User Interface Updates

To support this feature, the **Encryption settings for external database** section has been added to the **Compliance Settings Configuration** window. This set of fields appears only if you configure the **Message Archiver** and select a Microsoft SQL Server compliance database. This section contains the following fields, all of which are added for this release:

- **Enable Encryption on this cluster**—Check this check box to enable encryption in the local cluster
- **Enable Encryption on Remote Clusters**—Check this check box to enable encryption on intercluster peers in an intercluster network. The local cluster becomes the master cluster, which syncs its encryption key to the remote clusters, which are slave clusters.
- **Password/Confirm Password**—Enter the encryption password. You will need to reenter this password if you want to download the encryption key, disable encryption, or change the encryption password.
- **Status table for this cluster**—This read-only status table displays the status of any intercluster syncs, and which also displays which cluster is the master cluster. The table displays the following status columns:
  - Successful Modification Date—The result of the last successful configuration modification for both encryption passwords, and encryption status.
  - Failed Modification Date—If any attempts to change the encryption password or encryption status failed, the results display here.
  - Master Cluster ID—This field identifies which cluster, in an intercluster peer setup, is the master cluster.
- **Change Password**—If encryption is configured, click this button to change the password. You can only change the password on the master cluster.

- **Download Encryption Key**—Click this button to download the encryption key. To download the key, you must enter the encryption password as well as the public key that you generated with the external Windows tool.
- **Disable Encryption**—Check this check box to disable encryption.

Alarm Updates

The **MAencryptionMultiMaster** alarm has been added under the Cisco XCP Message Archiver service to indicate an issue with message archiver encryption. This alarm will be raised whenever you have an intercluster peer network where more than one cluster is configured as a master cluster for message archiver encryption.

Immediate Divert to Voicemail for WebEx Hybrid Services

The SIP trunk messaging specifications are updated to provide support for Immediate Divert to Voicemail from Cisco Webex Hybrid Services. To support this feature on Cisco Webex Hybrid Services, the SIP 603 DECLINE response has been added to the SIP trunk messaging specifications for Cisco Unified Communications Manager.

This update applies only for incoming calls to a Cisco Spark Remote Device. Previously, when a user declined an incoming call to this device type, the call was redirected to the user's enterprise phone. With the 603 Decline response, declined calls can go directly to the user's voicemail.

For information on how to configure this feature for Cisco Webex Hybrid Services, refer to your Hybrid Services documentation.

Persistent Chat Support on Jabber Mobile

This release supports persistent chat rooms for Cisco Jabber on iPhone, iPad, and Android. This update allows Cisco Jabber mobile clients to enjoy the exact same persistent chat functionality as desktop clients such as Cisco Jabber on Windows or Mac.

This feature includes no changes to the way persistent chat rooms are configured on the IM and Presence Service. However, the feature includes the following updates for Cisco Jabber on iPhone, iPad, and Android:

- Cisco Jabber mobile clients can now enter persistent chat rooms.
- The Mute function, which can be used to disable persistent chat notifications while Jabber is in silent mode. The Mute feature must be enabled by Cisco Jabber users from within their Cisco Jabber client.
- The Mentions feature, which overrides the Mute setting. If a Jabber user is mentioned, they will receive a notification, regardless of whether they've activated the Mute feature.
- Behind the scenes notifications to your other Jabber applications so that when you read a chat message on one device, it appears as a read message for all of your Jabber applications.

Minimum Release Support

The following minimum release support information applies for this feature:

Product	Support Information
IM and Presence Service	• For the 11.x set of releases, this feature is introduced with 11.5(1)SU5. For the 12.x set of releases, this feature will be introduced with 12.5(1). • If you have this feature deployed in 11.5(1)SU5 and you want to upgrade to a 12.x release, you must upgrade to 12.5(1) to maintain support for this feature. Persistent Chat for Jabber mobile clients is not supported with Release 12.0(1) or 12.0(1)SU1.
Cisco Jabber	• The minimum Cisco Jabber release is 12.1(0). • For additional information on Cisco Jabber functionality, refer to your Cisco Jabber documentation.

Configuration

For details on how to configure Persistent Chat, refer to the "Configure Chat Rooms" chapter of the *Configuration and Administration Guide for the IM and Presence Service*.

Push Notifications Updates

With this release, the behavior of the **Send Troubleshooting Information to Cisco Cloud** check box in the **Cisco Cloud Onboarding** window for the Push Notifications feature has changed as follows:

- Usage Metrics—With this release, Push Notifications usage metrics are now sent to the Cisco cloud once every 24 hours irrespective of the setting of this field. In previous releases, Push Notifications usage metrics were sent to the Cisco cloud only if this check box was checked. Usage metrics consists of the number of successful and failed Push Notifications–no user-generated content, or personally identifiable information, is passed along with these metrics.
- Default Setting—The default setting for this check box is checked. Previously, the default setting was unchecked.
- Alarms—There is no change to the behavior for Push Notifications alarms. Push Notifications alarms will be sent to the Cisco cloud only if this check box is checked.

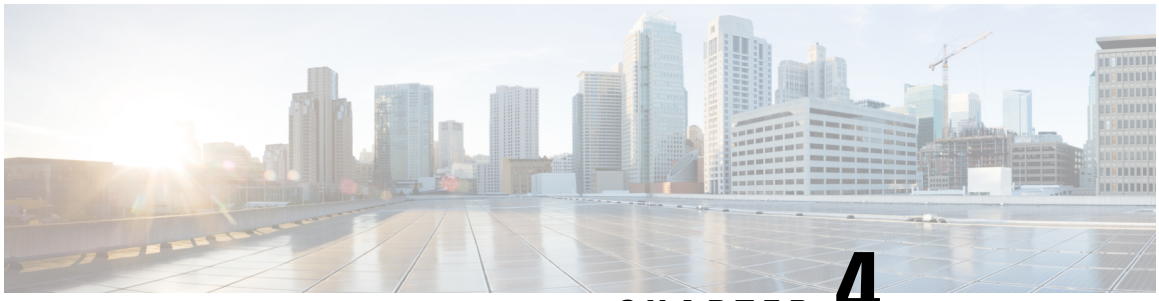
Search Conference Rooms via UDS Proxy for LDAP

As a part of this release, UDS Proxy feature is enhanced to support conference rooms represented as Room objects search in OpenLDAP Server. When no filter is set and the directory server type is OpenLDAP, Unified Communications Manager searches for users only using the default filter string (objectclass=inetOrgPerson). To search conference rooms, configure the custom filter with filter string (|(objectClass=intOrgPerson)(objectClass=rooms)) and use this custom filter in LDAP Search Settings.

This allows Cisco Jabber client to search conference rooms by their name and dial the number associated with the room. Conference rooms are searchable provided givenName, sn (lastName), mail, displayName, or telephonenumber attribute is configured in the OpenLDAP server for a room object.

This feature enhances the existing tokenizing rule for **name** search with search string containing multiple words with spaces. For example, when searching for a string A B C D with three spaces:

1. Searches the entire string (A B C D) as the First name.
2. Searches the entire string (A B C D) as the Last Name.
3. Searches the first word (A) as First Name and the remaining words (B C D) as the Last Name.
4. Searches the first word (A) as Last Name and the remaining words (B C D) as the First Name.



CHAPTER 4

Important Notes

- Features and Services, on page 27
- Interoperability, on page 28
- IM and Presence Service, on page 30
- Block Message Delivery Not Supported, on page 30
- Miscellaneous, on page 31

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

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 Cisco 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 12: 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 13: 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 14: 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.