Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1)SU3

First Published: 2020-08-13

Last Modified: 2021-04-29

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CONTENTS

CHAPTER 1

About this Release

About Release Notes

This release describes new features, restrictions, and caveats for Cisco Unified Communications Manager (Unified Communications Manager) and Cisco Unified Communications Manager IM and 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 software versions apply to Release 12.5(1)SU3:

- Unified Communications Manager: 12.5.1.13900-152
- IM and Presence Service: 12.5.1.13900-17

Version Compatibility Between Unified CM and the IM and Presence Service

Version compatibility depends on the IM and Presence Service deployment type. The following table outlines the options and whether a release mismatch is supported between the telephony deployment and the IM and Presence Service deployment. A release mismatch, if it is supported, would let you deploy your Unified Communications Manager telephony deployment and your IM and Presence Service deployment using different releases.

Note Any respin or ES that is produced between Cisco.com releases is considered part of the previous release. For example, a Unified Communications Manager ES with a build number of 12.5.1.18[0-2]xx would be considered part of the 12.5(1)SU7 (12.5.1.17900-x) release.

For Release 12.5(1)SU7a, a Unified Communications Manager ES with a build number of 12.5.1.181xx would be considered part of the 12.5(1)SU7a (12.5.1.18100-x) release.

Table 1: Version Compatibility between Unified Communications Manager and the IM and Presence Service

Deployment Type	Release Mismatch	Description
Standard Deployment of IM and Presence Service	Not supported	Unified Communications Manager and the IM and Presence Service are in the same cluster and must run the same release—a release mismatch is not supported.
Centralized Deployment of IM and Presence Service	Supported	The IM and Presence Service deployment and the telephony deployment are in different clusters and can run different releases—a release mismatch is supported. **Note** The IM and Presence Service central cluster also includes a standalone Unified CM publisher node for database and user provisioning. This non-telephony node must run the same release as the IM and Presence Service. **Note** Centralized Deployment is supported for the IM and Presence Service from Release 11.5(1)SU4 onward.

Documentation for this Release

For a complete list of the documentation that is available for this release, see the Documentation Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1).

Documentation Restructure 12.5(1)SU1 and Later

Following is a summary of the documentation restructure effort that was a part of 12.5(1)SU1. For this release and later releases, many Unified Communications Manager documents were restructured in order to improve usability and to streamline the documentation set. As part of this effort, one new guide is added, three existing guides are reworked, and five existing guides are deprecated. This overall effort reduces the size of the Unified Communications Manager documentation suite by four guides.

Table 2: Restructured Documents for 12.5(1)SU1 and Later

Restructured Documents	Deprecated Documents
Restructured Documents (Existing): • System Configuration Guide • Feature Configuration Guide • Administration Guide • Security Guide • Push Notifications Deployment for Cisco Jabber on iPhone and iPad **New Documents**: • Call Reporting and Billing Administration Guide	The following documents are deprecated for 12.5(1)SU1 and later: • *Cisco Unified CDR Analysis and Reporting Administration Guide*—Material moved to call reporting and billing documentation • *Call Detail Records Administration Guide*—Material moved to call reporting and billing documentation • *Cisco Unified Reporting Administration Guide*—Material is now with administration Guide • *Cisco Unified Serviceability Administration Guide*—Most sections are now in the Administration Guide. CDR Repository Manager and billing server sections are with call reporting and billing documentation • *Changing the IP Address, Hostname and Domain*—Material moved to the Administration Guide

System Configuration Guide (Restructured)

As of 12.5(1)SU1, the *System Configuration Guide* is shortened and streamlined to create a complete post-install system setup. Basic security and SSO configurations are added to fill out the basic setup, while advanced call processing features are moved to the *Feature Configuration Guide*. This new guide forms the Unified Communications Manager prerequisite for deploying an advanced Cisco call processing solution.

Administration Guide (Restructured)

As of 12.5(1)SU1, the *Administration Guide for Cisco Unified Communications Manager* is expanded to include consolidated administration information from the *Changing the IP Address, Hostname and Domain*document, the *Cisco Unified Reporting Administration Guide* document and many sections from the existing *Cisco Unified Serviceability Administration Guide* documentation, all of which are deprecated for 12.5(1)SU1 and later.

In addition to the above updates, an overview of troubleshooting information has been inserted into the *Administration Guide*.

Call Reporting and Billing Administration Guide (New document)

This new document simplifies call reporting and billing administration documentation, consolidating existing material from the documents *Cisco Unified CDR Analysis and Reporting Administration Guide* and the *Call Detail Records Administration Guide*, both of which are now deprecated. It also adds CDR Repository and billing server information that was available previously with the Serviceability documentation. The new guide simplifies the overall structure and provides a clearer setup process:

Feature Configuration Guide (Restructured)

This guide is expanded as the following advanced call processing topics are moved to this guide from the *System Configuration Guide*:

- Call Control Discovery
- External Call Control

- Call Queuing
- Call Throttling
- Logical Partitioning
- Location Awareness
- Flexible DSCP Marking and Video Promotion
- SIP Normalization and Transparency
- SDP Transparency Profiles
- Mobile and Remote Access

In addition, the following new sections are added for 12.5(1)SU1 and later:

- Headsets Management
- Headset Services
- Video Endpoints Management

Security Guide (Restructured)

The Security Guide is restructured for Release 12.5(1)SU3. The new guide is streamlined and enhanced to make it easy to configure and deploy security for Unified Communications Manager and registered endpoints. The new guide is split into three sections:

- **Basic Security**—Contains information on how to configure basic security on Unified Communications Manager and on registered endpoints.
- **User Security**—Contains information on how to manage identity, authentication, and user access.
- **Advanced Security Features**—Contains information on how to deploy advanced security features such as FIPS Mode, Enhanced Security Mode, and V.150.

The book also includes enhanced information with new topics on subjects like Security Hardening and Identity Management that help you make security decisions for your deployment.

Push Notifications Deployment for Cisco Jabber on iPhone and iPad (Revised)

This document describes how to configure Push Notifications for Cisco Jabber on iPhone and iPad with Cisco Unified Communications Manager and the IM and Presence Service. The guide is updated to include Push Notifications support for Cisco Jabber and Cisco Webex clients that run on both Android devices and iOS devices.

Open Source Documentation

This guide details the latest licenses and notices for the open source software used in Unified Communications Manager.

For more information on the open source softwares used, see https://www.cisco.com/c/dam/en_us/about/doing_business/open_source/docs/UnifiedCommunicationsManagerOpenSourceGuide1251SU3v10.pdf.

Installation Procedures

For information on how to install your system, see the Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1).

Upgrade Procedures

For information on how to upgrade to this release, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 12.5(1).

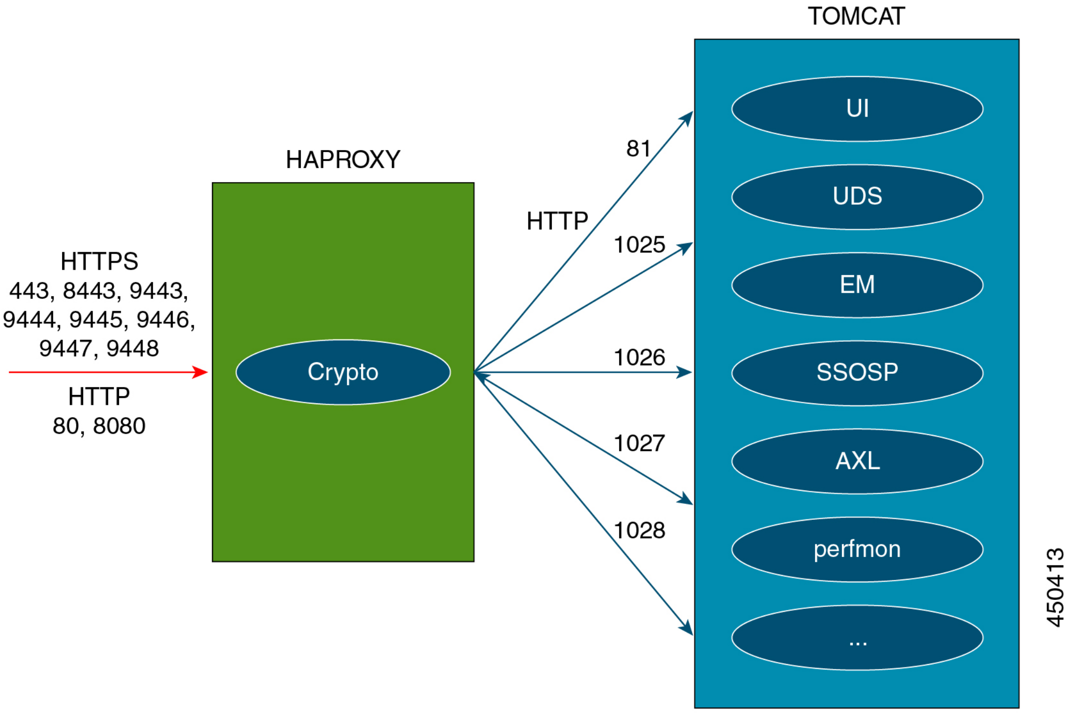
Meltdown Vulnerabilities During Upgrade

This release of Unified Communications Manager, Cisco IM and Presence Service, Cisco Emergency Responder, and Cisco Prime Collaboration Deployment contain software patches to address the Meltdown and Spectre microprocessor vulnerabilities.

Before you upgrade to Release 12.5(1) or above, we recommend that you work with your channel partner or account team to use the Cisco Collaboration Sizing Tool to compare your current deployment to an upgraded 12.5(1)SU3 deployment. If required, change VM resources to ensure that your upgraded deployment provides the best performance.

HAProxy—System Architecture Improvements for Web Traffic

HAProxy is a fast and reliable solution that offers high availability, load balancing, and proxy capabilities for HTTP-based applications. With this release, HAProxy frontends all the incoming web traffic into Unified Communication Manager and IM and Presence Service.



The HAProxy implementation has resulted in the following improvements:

- For about 10,000 client logins into Unified Communications Manager, there is an average of 30-40% improvement in the total time taken for clients to log in to the system.
- On an average, for 15,000 IM and Presence Service users, there is a 25-30% improvement in the total time taken for clients to log in to the system.
- The time taken to download the configuration files (includes phones and headset configuration file) for 10,000 devices has seen an average of 20-25% improvement.
- New Performance counters are introduced in Real Time Monitoring Tool (RTMT) for better troubleshooting and monitoring.
- Improved Tomcat stability through offloading of crypto functionality.

HAProxy Considerations

- Whenever the total CPU utilization crosses the 90% mark, HAProxy may trigger a service alarm along with the other services.
- Restart of the Cisco Tomcat service will internally restart the HAProxy service.

CHAPTER 2

New and Changed Features

Emergency Call Routing Regulations

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

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

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

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

Enhancement to Caller-ID in Call Pickup Notification Toast for Jabber in Deskphone Control Mode

The Caller ID is not shown in the Call Pickup notification toast when Cisco Jabber is in Deskphone control mode and Call Pickup page is configured to not show the caller ID. This makes the experience comparable to Jabber in softphone mode.

Extension Mobility Login Simplification using Headset

The Extension Mobility using headset feature that was introduced in Release 11.5(1)SU8 is carried over to 12.5(1)SU3 release. The following are additional updates introduced in this release:

- Administrator can associate headset to users from the Headset Inventory page.
- There is an administrator-controlled option to log in to Extension Mobility service using the headset without requiring a user PIN. This enables touchless login to the Extension Mobility service.

For more information, see 'Enable Pinless Extension Mobility Login' and 'Associate Phone Owner as Headset Owner' sections of the 'Headset Service' chapter in Feature Configuration Guide for Cisco Unified Communications Manager.

User Interface Updates

To support this feature, the following parameter and options are added:

1. In the **System** > **Enterprise Parameters Configuration** page, a new parameter **PIN entry for headset-based sign in** is added to enable or disable pinless Extension Mobility login.

   The following options are available in the new parameter:

   - Required
   - Not Required

2. In the **Device** > **Headset** > **Headset Inventory** page, two new options are added to associate or disassociate bulk headsets to the user.

   The following are the options:

   - Associate Phone Owner as Headset Owner
   - Disassociate Headset Owner

Connected Number Display for Forwarded Calls for Jabber in Deskphone Control Mode

In this release, Cisco Jabber in Deskphone control mode honors the "Always Display Original Dialed Number" Service Parameter configured in the Cisco Unified Communication Manager Administration user interface.

When this parameter is configured, original dialed number is displayed as connected number on caller's display. This ensures that user's privacy settings are honored.

Granular Access Control Enhancements

Granular Access Control Enhancements allows creation of hierarchy among administrators for segregation of duties. This enhancement allows the higher ranked user to view or modify the permission information or user rank of same or lower ranked users but not vice versa.

User Interface Updates

The following fields are introduced:

- In the **User Management > User Settings > Roles** page, two new fields are added under the **Advanced Role Configuration** window.
  - **User can update Permissions Information for own user**
  - **User can update User Rank for own user**

For more information, see the *Cisco Unified CM Administration Online Help*.

Native Phone Migration using IVR and Phone Services

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

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

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

Table 3: Different Phone Migration Options and Considerations

	Using Self-provisioning IVR Service	Using Phone Migration Service	Using Unified CM Administration Interface
End user or administrator driven phone migration	End user (Self-service)	End user (Self-service)	Administrator
Auto-registration required	Yes	No	No

	Using Self-provisioning IVR Service	Using Phone Migration Service	Using Unified CM Administration Interface
Migration steps	• Auto register a new phone • Dial self-provisioning IVR number • Follow the voice prompts	• Plug-in new phone to the network • Key in primary extension and PIN (optional)	• Sign in to Cisco Unified CM Administration interface • Choose "Migrate Phone" option in the Phone Configuration page of the old phone • Enter phone type (model & protocol) and MAC address of the new phone
Administrator involvement	Medium	Low	High

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

User Interface Updates

The following fields are added:

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

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

BFCP Presentation Sharing in Audio Only Call with TRP

Unified Communication Manager supports BFCP-based presentation sharing when two video capable devices start a call in Audio Only mode and there is a TRP in the media path.

For more information, see the “Configure Presentation Sharing using BFCP” chapter in the Feature Configuration Guide for Cisco Unified Communications Manager.

Push Notifications for iOS and Android Clients

This release includes a number of updates and changes for Push Notifications deployments.

Apple Push Notifications Updates

As of August 2020, legacy VoIP mode is now disabled for Cisco Jabber on iPhone and iPad clients, making Push Notifications a mandatory deployment for Cisco Jabber on iPhone and iPad clients.

Apple Push Notifications support for Cisco Jabber and Cisco Webex clients that run on iOS devices is updated to meet new Apple requirements and also to support iOS 13 SDK updates. Updates include:

- Caller ID in the Push Notifications–Cisco Jabber and Cisco Webex clients now launch CallKit with Caller ID once the Push Notification is received, rather than when the SIP INVITE is received. The Caller ID supports External Presentation Name and Number, if it is configured on Unified Communications Manager.
- Active Registration node—Push Notifications now include the IP address of the node which generates the Push Notification. This update prevents delay in registration if the node to which the client was registered previously restarts while the client is in the background. With this change, the client can quickly register to the node that generates Push Notification and is in a healthy state.
- Push Notifications support in China—This release supports changes that are required for Apple devices in the China region so that the Cisco Jabber or the Cisco Webex client complies with local government regulations about VOIP applications not showing CallKit. Note that Cisco Jabber version 12.9MR is required for users in China Region.

Note These updates assume that you have updated Cisco Jabber to 12.9. If you are running earlier Jabber versions, Push Notification will not include the Apple Push Notification service changes that are included in iOS 13.

For more information on iOS 13 requirements for Push Notifications, see the section Apple Push Notifications Service Updates.

Android Push Notifications Support Introduced

This release introduces Push Notifications support for Cisco Jabber and Cisco Webex clients that run on Android devices. Android Push Notifications feature support includes:

- Active Registration node—Push Notifications include the IP address of the node which generates the Push Notification. This update prevents a delay in registration if the node to which the client was registered previously restarts while the client is in background mode. With this change, the client can quickly register to the node that generates the Push Notification and is in a healthy state.

Note For Cisco Webex clients, only voice push notifications are supported.

Note Android Push Notifications do not support Caller ID within the Push Notification. The CallKit launches only when the client receives the SIP INVITE. In addition, Android Push Notifications are not supported in China.

Push Notifications Deployment and Configuration

For detailed information on how to deploy and configure Push Notifications for either Android or iOS clients, see the Push Notifications Deployment Guide.

IM and Presence Configuration for SIP Open Federation

Cisco IM and Presence Service supports SIP open federation for Cisco Jabber clients. As an administrator, you can configure SIP open federation allowing Cisco Jabber users to seamlessly federate with users from domains that support SIP based federation. This feature establishes the co-existence of open IM federation for both SIP and XMPP clients in the IM and Presence server. Unlike in Controlled SIP Federation where you must configure each federated domain separately, you can configure open federation for all domains with a single pre-configured static route. The static route lets Cisco Jabber federate with any external domain. More importantly, it significantly cuts down the time to configure and maintain SIP federation for individual domains.

For configuration information, see the "IM and Presence Configuration for SIP Open Federation" chapter in the Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager Guide.

IM and Presence Intercluster Peer Synch Interval

IM and Presence Service allows you to set time interval for intercluster peer syncing. The newly introduced service parameter **Inter Cluster Peer Periodic Sync Interval (mins)** allows you to configure the time interval for dynamic ICSA periodic sync from **Cisco Unified CM IM and Presence Administration** user interface. If the intercluster peer sync fails, then ICSA service restarts.

For detailed information on how to configure intercluster peer sync interval, see chapter 'Configure Intercluster Peers' in Configuration and Administration of the IM and Presence Service.

CHAPTER 3

Important Notes

Default CA Certificates During New Install and Upgrades

After you install Unified Communications Manager Release 12.5(1) and above, all of the default CA certificates except for the CAP_RTP_001 and CAP_RTP_002 certificates are present. You can enable these certificates using the **set cert default-ca-list enable { all | common-name }** command.

If you are upgrading to Unified Communications Manager Release 12.5(1) and above, only the default certificates that were present in the older version appear after the upgrade.

Disabled Default Certificates Backup Fails

When you perform a backup using Disaster Recovery System (DRS), if all or specific default certificates are disabled using **set cert default-cal-list disable {all | common-name}**, then backup does not contain disabled certificates. When you are restoring the backup on the fresh installed server, those disabled certificates reappear.

ILS Networking Capacities

The Intercluster Lookup Service (ILS) network capacities have been updated for Release 12.5(x) and up. Following are the recommended capacities to keep in mind when planning an ILS network:

- ILS networking supports up to 10 hub clusters with 20 spoke clusters per hub, up to a 200 total cluster maximum. A hub and spoke combination topology is used to avoid many TCP connections created within each cluster.
- There may be a performance impact with utilizing your hub and spoke clusters at, or above, their maximums. Adding too many spoke clusters to a single hub creates extra connections that may increase the amount of memory or CPU processing. We recommend that you connect a hub cluster to no more than 20 spoke clusters.
- ILS networking adds extra CPU processing to your system. When planning your hub and spoke topology, make sure that your hub clusters have the CPU to handle the load. It may be a good idea to allocate systems with high CPU utilization as spoke clusters.

Note The above capacities are recommendations only, based on system testing. Unified Communications Manager does not enforce a limit, either on the total number of clusters in an ILS network, or on the number of spoke clusters per hub. The above topology is tested to ensure optimum performance so that the system does not burn too many resources.

For additional information on ILS, see the 'Configure Intercluster Lookup Service' chapter in the System Configuration Guide for Cisco Unified Communications Manager.

Java Requirements for SAML SSO Login to RTMT via Okta

If you have SAML SSO configured with Okta as the identity Provider, and you want to use SSO to log in to the Cisco Unified Real-Time Monitoring Tool, you must be running a minimum Java version of 8.221. This requirement applies to 12.5(x) releases of Cisco Unified Communications Manager and the IM and Presence Service.

Multiple Clock-Rates Not Supported in Same Call

With this release, Cisco TelePresence endpoints and Cisco Jabber clients do not support multiple “Telephone-Event” SDP attributes with different clock rates to match the offered codecs. This capability is required to interwork with VoLTE/IMS endpoints fully. Due to this update, interoperability issues between these endpoint types and VoLTE or IMS endpoints may arise for mid-call reinvites where a different clock rate from 8 kHz is negotiated.

For calls between these endpoint classes:

- The initial call setup occurs without any issues.
- Mid-call Re-INVITE will see no issues if the invite is initiated by Unified Communications Manager.
- Endpoint-initiated reinvites may see interoperability issues if they use a different clock-rate than 8 kHz.

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 4: 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 5: 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

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

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.

Export Control with Satellite Deployment for Export Restricted Customer

Unified Communications Manager supports Export Restricted Customers to enable Export Control functionality on Unified Communications Manager with Satellite Deployment (Satellite Version: 7-202001). See the 'Smart Software Licensing Overview' section in the "Smart Licensing Export Compliance" chapter of the System Configuration Guide for Cisco Unified Communications Manager. For more information on Satellite, see https://software.cisco.com/download/home/286285506/type/286285517/os.

Upgrade Database Schema from IM and Presence Release 11.5(1) and Above

If you have Microsoft SQL database deployed as an external database with the IM and Presence Service, choose either of the following scenarios to upgrade the database schema.

Table 6: MSSQL Database Schema Upgrade Scenarios

Scenario	Procedure
Upgrade from IM and Presence Service 11.5(1), 11.5(1)SU1, or 11.5(1)SU2 release	For more information on how to upgrade your MSSQL database, see the 'Database Migration Required for Upgrades with Microsoft SQL Server' section in the Database Setup Guide for the IM and Presence Service. This makes the necessary changes to the column types from TEXT to nvarchar(MAX).

Scenario	Procedure
Upgrade from IM and Presence Service 11.5(1)SU3 or later	The MSSQL database connected to the IM and Presence Service Server is upgraded automatically during IM and Presence Service upgrade. This makes the necessary changes to the column types from nvarchar(4000) to nvarchar(MAX). **Note** If you want to trigger an upgrade manually for any reason, such as to connect to an older database with column type as nvarchar(4000), the following actions trigger and upgrade the database by changing the column type to nvarchar(MAX): • Restarting Cisco XCP Config Manager followed by restarting Cisco XCP Router service; or • During schema verification of the external database—when you assign the database to Text Conferencing (TC), Message Archiver (MA) or Asynchronous File transfer (AFT) services, and reload the **External Database Settings** page. (From the Cisco Unified CM IM and Presence Administration user interface, choose **Messaging** > **External Server Setup** > **External Databases**, and then find and select the database to load the **External Database Settings** page.)

Unresponsive Remote Cluster Nodes

Problem

All nodes of the remote cluster are down at once.

Description

If in the preceding problem,

- We have two clusters with four nodes each and all nodes on both clusters are UDS configured.
- Cluster 2 is defined under Cluster 1 view with Publisher FQDN and conversely, the Jabber user has home cluster as Cluster 1 but SRV points to Cluster 2, then Cluster 2 holds all the entries of `RemoteClusterServiceMapDynamic` table that are initially updated when FQDN of Publisher from Cluster 1 is configured under Cluster View was reachable.
- If all three nodes of Cluster 1 under `RemoteClusterServiceMapDynamic` of Cluster 2 are down at once due to an outage, the new Jabber login fails to discover the home Cluster.
- Even when the nodes are down, `RemoteClusterServiceMapDynamic` on Cluster 2 continues to display the previous IPs.
- Cluster 2 automatically updates the entry of the next node in the list with UDS active, if the nodes are brought down sequentially or one node from `RemoteClusterServiceMapDynamic`, goes down.

The problem is when all 3 nodes from Cluster 1 which are under `RemoteClusterServiceMapDynamic` are down due to an outage, the 4th node doesn't get added to `RemoteClusterServiceMapDynamic`. However, if you point a responsive Cluster View of Cluster 2 to an active Subscriber on Cluster 1, then `RemoteClusterServiceMapDynamic` is updated automatically.

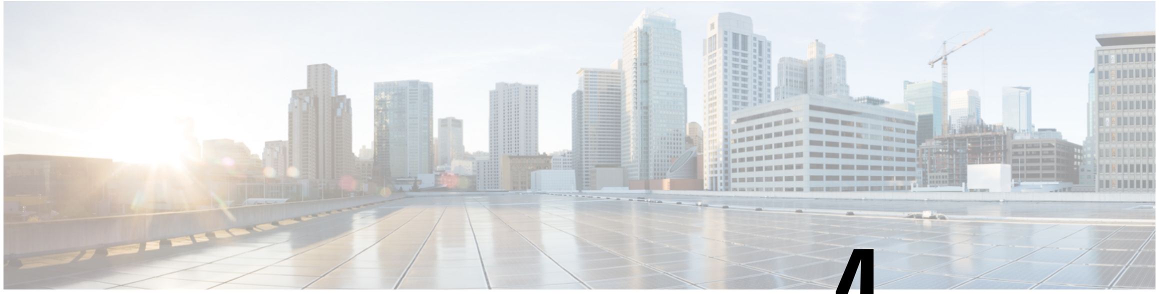
Solution

Delete the inactive remote node from the cluster view and add an active node.

This update is a part of CSCvq5867

Restart Cisco Tomcat Service

We recommend that you restart the Cisco Tomcat service after enabling or disabling Security Assertion Markup Language Single Sign-On (SAML SSO).



CHAPTER 4

Caveats

Bug Search Tool

The system grades known problems (bugs) per severity level. These release notes contain descriptions of the following bug levels:

- All severity level 1 or 2 bugs
- Significant severity level 3 bugs
- All customer-found bugs

You can search for open and resolved caveats of any severity for any release using the Cisco Bug Search tool, an online tool available for customers to query defects according to their own needs.

To access the Cisco Bug Search tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Follow these steps to use Cisco Bug Search tool:

1. Access the Cisco Bug Search tool: https://tools.cisco.com/bugsearch/.
2. Log in with your Cisco.com user ID and password.
3. If you are looking for information about a specific problem, enter the bug ID number in the **Search for:** field and click **Go**.

Tip Click **Help** on the Bug Search page for information about how to search for bugs, create saved searches, and create bug groups.

Caveats for 12.5(1)SU3

The following table compiles open caveats in this release. You can search for defects in the Bug Search Tool at https://bst.cloudapps.cisco.com/bugsearch/.

Caveats for 12.5(1)SU3

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

- ReadMe for Cisco Unified Communications Manager Release 12.5(1)SU3
- ReadMe for Cisco Unified IM and Presence, Release 12.5(1)SU3