



Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1)SU4

First Published: 2021-02-22

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 NON-INFRINGEMENT 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1

About this Release 1

About Release Notes 1

Supported Versions 1

Version Compatibility Between Unified CM and the IM and Presence Service 1

Documentation for this Release 2

Documentation Restructure 12.5(1)SU1 and Later 2

Installation Procedures 4

Upgrade Procedures 4

Meltdown Vulnerabilities During Upgrade 4

CHAPTER 2

New and Changed Features 5

Headset and Accessories Inventory Download 5

Oracle JRE Removal from Manager Assistant 5

Smart Licensing Registration Through Authentication Based Proxy 6

SSO Redirect URI for Webex Apps 6

Performance Counters for Mobile and Remote Access Device Registrations 6

UDS Enhancements 6

Certificate Sync and Intercluster Periodic Sync 7

Improved IM and Presence Stream Features/Services Advertisement via Expressway 7

CHAPTER 3

Important Notes 9

Default CA Certificates During New Install and Upgrades 9

Disabled Default Certificates Backup Fails 9

ILS Networking Capacities 9

Java Requirements for SAML SSO Login to RTMT via Okta	10
Multiple Clock-Rates Not Supported in Same Call	10
New Cisco Gateway Support	10
SDL Listening Port Update Requires CTIManager Restart on all Nodes	12
Export Control with Satellite Deployment for Export Restricted Customer	12
Upgrade Database Schema from IM and Presence Release 11.5(1) and Above	12
Unresponsive Remote Cluster Nodes	13
Restart Cisco Tomcat Service	14

CHAPTER 4**Caveats 15**

Bug Search Tool	15
Caveats for 12.5(1)SU4	16



CHAPTER 1

About this Release

- [About Release Notes, on page 1](#)
- [Supported Versions, on page 1](#)
- [Documentation for this Release, on page 2](#)
- [Installation Procedures, on page 4](#)
- [Upgrade Procedures, on page 4](#)

About Release Notes

These release describe 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)SU4:

- Unified Communications Manager: 12.5.1.14900-63
- IM and Presence Service: 12.5.1.14900-4

Version Compatibility Between Unified CM and the IM and Presence Service

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

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	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	Supported	<p>The IM and Presence deployment and the telephony deployment are in different clusters and can run different releases—a release mismatch is supported.</p> <p>Note The IM and Presence 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.</p> <p>Note Centralized Deployment is supported for the IM and Presence Service from Release 11.5(1)SU4 onward.</p>

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	Description
System Configuration Guide	As of 12.5(1)SU1, the <i>System Configuration Guide</i> 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 <i>Feature Configuration Guide</i> . This new guide forms the Unified Communications Manager prerequisite for deploying an advanced Cisco call processing solution.

Restructured Documents	Description
Feature Configuration Guide	<p>This guide is expanded as the following advanced call processing topics are moved to this guide from the <i>System Configuration Guide</i>:</p> <ul style="list-style-type: none"> • 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 <p>In addition, the following new sections are added for 12.5(1)SU1 and later:</p> <ul style="list-style-type: none"> • Headsets Managements • Video Endpoints Management
Administration Guide	<p>As of 12.5(1)SU1, the <i>Administration Guide for Cisco Unified Communications Manager</i> is expanded to include consolidated administration information from the <i>Changing the IP Address, Hostname and Domain</i> document, the <i>Cisco Unified Reporting Administration Guide</i> document and many sections from the existing <i>Cisco Unified Serviceability Administration Guide</i> documentation, all of which are deprecated for 12.5(1)SU1 and later.</p> <p>In addition to the above updates, an overview of troubleshooting information has been inserted into the <i>Administration Guide</i>.</p>
Call Reporting and Billing Administration Guide	<p>This new document simplifies call reporting and billing administration documentation, consolidating existing material from the documents <i>Cisco Unified CDR Analysis and Reporting Administration Guide</i> and the <i>Call Detail Records Administration Guide</i>, 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:</p>

Table 3: Restructured Documents for 12.5(1)SU3 and Later

Restructured Documents	Description
Security Guide	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
Push Notifications Deployment for Cisco Jabber on iPhone and iPad	<p>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.</p>

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)SU4 deployment. If required, change VM resources to ensure that your upgraded deployment provides the best performance.



CHAPTER 2

New and Changed Features

- [Headset and Accessories Inventory Download](#), on page 5
- [Oracle JRE Removal from Manager Assistant](#), on page 5
- [Smart Licensing Registration Through Authentication Based Proxy](#), on page 6
- [SSO Redirect URI for Webex Apps](#), on page 6
- [Performance Counters for Mobile and Remote Access Device Registrations](#), on page 6
- [UDS Enhancements](#), on page 6
- [Certificate Sync and Intercluster Periodic Sync](#), on page 7
- [Improved IM and Presence Stream Features/Services Advertisement via Expressway](#), on page 7

Headset and Accessories Inventory Download

The **Headsets** menu category is renamed to **Headsets and Accessories** in the Cisco Unified Communications Manager user interface.

This feature enables an administrator to download a detailed report of Headsets and Accessories in your deployment into a CSV file from the Unified Communications Manager user interface.

For more information, see the “Headset and Accessories Management” chapter in the [Feature Configuration Guide for Cisco Unified Communications Manager](#).

Oracle JRE Removal from Manager Assistant

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

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

- Uninstall the Cisco Unified Communications Manager Assistant client that is currently installed on your machine.
- Install JRE on 32-bit or 64-bit Windows platform.

For more information, see the [Feature Configuration Guide for Cisco Unified Communications Manager](#).

Smart Licensing Registration Through Authentication Based Proxy

This feature enables licensing component on Unified Communications Manager to communicate with the cloud-based Cisco Smart Software Manager using an authenticated connection through the HTTP/HTTPS proxy.

SSO Redirect URI for Webex Apps

As part of the SSO Redirect URI for Webex Apps feature, **Cisco Jabber** is replaced with **Client** to make it more generic as it's now supported by both **Cisco Jabber and Webex Apps**.

Webex Client Embedded Browser Support

This feature enhances the security of Cisco Jabber/Webex Client Embedded Browser Support.

Enhancements include:

- Protection against "*Authorization Code Interception Attack*", as per RFC7636.
- Improved calling experience prevents dual login when SSO is enabled while using Webex Client(s) or Unified Communications Manager.

Performance Counters for Mobile and Remote Access Device Registrations

New performance counters are introduced in the Cisco Unified Real-Time Monitoring Tool to track registered Cisco Webex App and Cisco Jabber devices registered to Unified Communication Manager in Mobile and Remote Access mode. This enables administrators to get insight into how many devices in Mobile and Remote Access mode are registered to Unified CM. When you enable troubleshooting perfmon data logging, system automatically collects statistics for these new counters and stores it in perfmon logs.

For more information on the new counters, see the [Cisco Unified Real-Time Monitoring Tool Administration Guide](#).

UDS Enhancements

The following enhancements are introduced for UDS:

- The UDS Bulk Search by Email enables Cisco Jabber to send requests in batches using the email attribute to prevent high CPU usage by UDS and Cisco Tomcat services.
- UDS is enhanced to do a better discovery of the home cluster of a user across remote clusters. This helps in avoiding the Cisco Jabber login failures and ensures geo redundancy in the event of Data Center failure or shutdown.

Certificate Sync and Intercluster Periodic Sync

The IM and Presence Service performs certificates sync as part of the intercluster sync process. This feature introduces a new service parameter **Certificate Sync during Inter-Cluster Periodic Sync** and allows the administrator to disable or enable certificates synchronization as part of Intercluster periodic sync from the Cisco Unified Communications Manager IM and Presence Administration user interface.

The Certificate Sync feature introduces the following options:

- **Perform certificate sync**—This is the default value of the **Certificate Sync during Inter-Cluster Periodic Sync** service parameter. When the **Certificate Sync during Inter-Cluster Periodic Sync** service parameter is set to **Perform certificate sync** and the certificates are not synchronized across the intercluster peers, it requires a Force Manual Sync operation to synchronize data and certificates.
- **Do not perform certificate sync**—To disable the certificate sync during the ICSA sync, the administrator can set the **Certificate Sync during Inter-Cluster Periodic Sync** service parameter to **Do not perform certificate sync**.

**Note**

If you encounter performance degradation or high CPU spikes in your deployment that is related to certificate sync during intercluster periodic sync, you can use this feature.

For detailed information on how to disable or enable certificates sync as part of the intercluster sync process, see chapter 'Configure Intercluster Peers' in the [Configuration and Administration of the IM and Presence Service Guide](#).

Improved IM and Presence Stream Features/Services Advertisement via Expressway

IM and Presence Service now supports the advertisement of XMPP stream features/services to the clients connecting over Cisco Expressway's Mobile and Remote Access.

This new functionality enables deployments with mixed IM and Presence Service versions, for example some clusters on 11.5(1)SU8 and some other clusters on 12.5(1)SU3, to work with Cisco Expressway so that Cisco Jabber clients can discover the correct capabilities applicable to it based on the IM and Presence Service home cluster it is assigned to.

For this mechanism to work, the minimum deployment requirement is to have Cisco Expressway running version X12.7 or higher and have at least one IM and Presence cluster in the intercluster mesh running version 11.5(1)SU9 or 12.5(1)SU4 and above.

Depending on your current IM and Presence Service version mix, you may need to enable or disable push notifications feature using FCM service flag on the Expressway as per the information given in the following table:

```
xConfiguration XCP Config FcmService: On/Off
```



Note Apple Push Notification Service (APNS) is not affected by the FCM service flag status.

Table 4: Solution Matrix from the Perspective of Expressway CLI Enable/Disable Command for Android Push Notifications (FCM)

Mixed Versions IM and Presence Clusters	Expected Status of FCM Flag on Expressway X12.7	Comment
Any 11.5(1)SU with 12.5(1)SU2 and lower	OFF	Android Push (FCM) NOT supported.
11.5(1)SU8 (and lower) or 12.5(1)SU2 (and lower) with 12.5(1)SU3	OFF	Android push (FCM) NOT supported
11.5(1)SU8 (and lower) or 12.5(1)SU2 (and lower) with 12.5(1)SU4 (and higher)	OFF	Android push (FCM) supported on 12.5(1)SU4 (or newer) versions
11.5(1)SU9 (and higher) or 12.5(1)SU4 (and higher) with 12.5(1)SU3	ON	Android push (FCM) supported on version 12.5(1)SU3 and higher
11.5(1)SU9 (and higher) with 12.5(1)SU4 (and higher)	Flag not required (Expressway 12.7 relies fully on the new discovery mechanism)	Android push (FCM) supported on 12.5(1)SU4 (or newer) versions



CHAPTER 3

Important Notes

- [Default CA Certificates During New Install and Upgrades](#), on page 9
- [Disabled Default Certificates Backup Fails](#), on page 9
- [ILS Networking Capacities](#), on page 9
- [Java Requirements for SAML SSO Login to RTMT via Okta](#), on page 10
- [Multiple Clock-Rates Not Supported in Same Call](#), on page 10
- [New Cisco Gateway Support](#), on page 10
- [SDL Listening Port Update Requires CTIManager Restart on all Nodes](#), on page 12
- [Export Control with Satellite Deployment for Export Restricted Customer](#), on page 12
- [Upgrade Database Schema from IM and Presence Release 11.5\(1\) and Above](#), on page 12
- [Unresponsive Remote Cluster Nodes](#), on page 13
- [Restart Cisco Tomcat Service](#), on page 14

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, refer to 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, 10.5(2) and 11.5(x)), support for the gateway model is added as of the specified release, along with later releases in that category. For these releases, you can select the gateway in the **Gateway Configuration** window of Unified Communications Manager.

Table 5: Cisco Gateways with Initial Release By Release Category

Gateway Model	10.5(2) Releases	11.5(x) Releases	12.0(x) Releases	12.5(x) Releases	14(x) Releases
Cisco VG 202, 202 XM, 204, 204 XM, 310, 320, 350 Analog Voice Gateway	10.5(2) and later	11.5(1) and later	12.0(1) and later	12.5(1) and later	14 and later
Cisco VG400 Analog Voice Gateway	Not supported	11.5(1)SU7 and later	12.0(1)SU2 and later	12.5(1) and later	14 and later
Cisco VG420 Analog Voice Gateway Note Cisco VG420 Analog Voice Gateway is expected to release in July 2021, dates are subject to change.	Not supported	11.5(1)SU9 and later	12.0(1)SU2 and later	12.5(1)SU4 and later	14SU1 and later
Cisco VG450 Analog Voice Gateway	10.5(2)SU8 and later	11.5(1)SU6 and later	12.0(1)SU2 and later	12.5(1) and later	14 and later
Cisco 4321, 4331 4351, 4431, 4451 Integrated Services Router	10.5(2) and later	11.5(1) and later	12.0(1)SU2 and later	12.5(1) and later	14 and later
Cisco 4461 Integrated Services Router	10.5(2)SU8 and later	11.5(1)SU6 and later	12.0(1)SU2 and later	12.5(1) and later	14 and later
Cisco 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 6: Cisco Analog Telephone Adapters

ATA Adapter	10.5(2)x Releases	11.5(x) Releases	12.0(x) Releases	12.5(x) Releases	14(x) Releases
Cisco ATA 190 Analog Telephone Adapter	10.5(2) and later	11.5(1) and later	12.0(1) and later	12.5(1) and later	14 and later
Cisco ATA 191 Analog Telephone Adapter	10.5(2)SU7 and later	11.5(1)SU4 and later	12.0(1)SU2 and later	12.5(1) and later	14 and later

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 7: MSSQL Database Schema Upgrade Scenarios

Scenario	Procedure
Upgrade from IM and Presence 11.5(1), 11.5(1)SU1, or 11.5(1)SU2 release	<p>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.</p> <p>This makes the necessary changes to the column types from TEXT to nvarchar(MAX).</p>
Upgrade from IM and Presence 11.5(1)SU3 or later	<p>The MSSQL database connected to the IM and Presence Server is upgraded automatically during IM and Presence upgrade. This makes the necessary changes to the column types from nvarchar(4000) to nvarchar(MAX)..</p> <p>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):</p> <ul style="list-style-type: none"> • 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](#), on page 15
- [Caveats for 12.5\(1\)SU4](#), on page 16

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)SU4

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)SU4

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

- [ReadMe for Cisco Unified Communications Manager Release 12.5\(1\)SU4](#)
- [ReadMe for Cisco Unified IM and Presence, Release 12.5\(1\)SU4](#)