Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1)SU5

First Published: 2021-08-03

Last Modified: 2023-08-03

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)SU5:

- Unified Communications Manager: 12.5.1.15900-66
- IM and Presence Service: 12.5.1.15900-5

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.

For Release 12.5(1)SU8, a Unified Communications Manager ES with a build number of 12.5.1.19[0-2]xx would be considered part of the 12.5(1)SU8 (12.5.1.18900-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	Description
System Configuration Guide	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.

Restructured Documents	Description
Feature Configuration Guide	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 Managements • Video Endpoints Management
Administration Guide	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	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:

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

Restructured Documents	Description
Security Guide	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	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.

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).

Side-channel 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)SU7 deployment. If required, change VM resources to ensure that your upgraded deployment provides the best performance.

New and Changed Features

Enhanced Security Compliance

As part of Cisco's continuous review of the Unified Communications Manager and IM and Presence Service architecture to identify security vulnerabilities and weaknesses, the following compliance and validation investments were made as part of the security compliance roll-out:

Cross-Site Scripting Vulnerability—A vulnerability in the web-based management interface is addressed so that it does not allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. Open Web Application Security Project (OWASP) encoding guidelines were implemented to fix the XSS vulnerabilities.

Also, heightened the security compliance measures to achieve Host header validation for the trusted list of hosts in Unified CM. Apart from the Referer header, Unified CM first validate the IP Address or Hostname present in the Host header with the servers configured in the Unified CM cluster. If no match is found, then an attempt to match the host value with the trusted list of hosts configured in the Cisco Unified CM Administration Enterprise Parameters page is completed before allowing access to Unified CM.

Fresh Install with Data Import

Virtual to Virtual (V2V) migration make it easy to upgrade and migrate Unified Communications Manager. In the same process, you can upgrade the Unified Communications Manager version, move to a new virtual machine configuration, migrate data between clusters, upgrade the VMware vSphere ESXi version, and migrate to new hardware if desired.

Fresh Install with Import Data also provides an alternative to Direct Refresh Upgrade and PCD Migration (for scenarios where temporary migration hardware or configuration of management applications is undesirable).

You can:

- Export data from an existing cluster to an SFTP server.
- Perform fresh installation of a new cluster and import data from the SFTP server into the new cluster. This can be done through the touchless installation as well. An option for data import appears in new sections of the install wizard and Answer File Generator.

For more information on Install with Data Import, see the Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service.

CLI Update

To support data export from your old system to the SFTP server, use the following commands:

- **utils system upgrade dataexport initiate**
- **utils system upgrade dataexport status**
- **utils system upgrade dataexport cancel**

For more details about the CLI commands, see the "Utils Commands" chapter in the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

Stronger Cipher Suites on CTI Ports

Unified Communications Manager provides a stronger cipher suite on the Skinny Client Control Protocol (SCCP) interface for CTI ports and allows secure media notification between the calling and called party. For more information, see the 'Stronger Cipher Suites on CTI Ports' section in Security Guide for Cisco Unified Communications Manager.

Implementation of Certificate Filename Change

This feature addresses the scenario where you cannot have multiple certificates from the same Certificate Authority with a similar name. The introduction of serial number along with the common name for the certificates identifies each certificate uniquely. The filename for the certificates are defined as **commoname_serialnumber.pem**. Since each certificate is different, you can upload more than one certificate from the same Certificate Authority.

The certificate filename changes will not affect any existing functionality and Intercluster Sync Agent (ICSA) works as earlier. The IM and Presence Service certificates, Unified Communications Manager certificates, and Third-party certificates that are uploaded from Unified Communications Manager and IM and Presence Service follows the new naming process and creates cache certificates with the new name.

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
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).
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 Managed File transfer (MFT) 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).

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)SU5

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)SU5

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

- ReadMe for Cisco Unified Communications Manager Release 12.5(1)SU5
- ReadMe for Cisco Unified IM and Presence, Release 12.5(1)SU5