Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 14SU1

First Published: 2021-10-27

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.

About this Release

The following software versions apply to Release 14SU1:

- Unified Communications Manager: 14.0.1.11900-132
- IM and Presence Service: 14.0.1.11900-9

Version Compatibility Between Unified CM and the IM and Presence Service

Version compatibility depends on the IM and Presence deployment type. 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.

Deployment Type	Release Mismatch	Description
Centralized Deployment of IM and Presence	Supported	The IM and Presence deployment and the telephony deployment are in different clusters and can run different releases—a release mismatch is supported. **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. **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 14.

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 14.

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 14.

New and Changed Features

Automated Installation using vApp properties and VMware OVF Tool

This feature eases installation using a skip-install Open Virtual Archive (OVA) file for Unified Communications Manager and IM and Presence Service clusters. The VMware OVF Tool is used to deploy and inject the Unified CM and IM and Presence Service configuration parameters into the virtual machines using skip-install OVA and vApp properties without using Answer File Generator or vFloppy images.

Fresh Install and Fresh Install with Data Import is supported using this method. You can deploy this installation in two ways:

- **Manual Installation Using vApp Options**—Deploy the skip-install OVA on each node in the cluster manually by logging into the respective VMware Embedded Host Client or vCenter Server, where the Unified CM server configurations can be entered.
- **Touchless Installation Using VM Tools**—Run the Cisco VM Builder tool (which is a VMware wrapper tool that is provided as part of the platform skip-install-ova rpm/tar) by passing the Unified CM configuration parameters, skip-install OVA, and VMware Embedded Host Client or vCenter Server details of each node in the cluster, which performs the complete cluster installation without manual intervention.

For more information on the installation procedures, see the 'Automated Installation using vApp properties and VMware OVF Tool' section in the Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service.

Enhanced Accessibility and Usability

The Cisco Unified CM Administration user interface and Self Care Portal are enhanced with the following accessibility improvements:

- Keyboard navigation—Better skip navigation support that allows users to bypass the menu/sub-menu content.
- Assistive fields—Notes, Hints, and required fields are added so that the screen readers can read them.
- High contrast mode—Contrast ratio and labeling are addressed across the Self Care Portal including Dialog Boxes and Pop-ups.
- Keyboard focus—Better focus using TAB keys in all the elements under **Phones > Call Forwarding** Menu in Self Care Portal.

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.

Opus Codec Transcoder Support

The Unified Communications Manager now includes Skinny Client Control Protocol (SCCP) controlled iOS-based registered media resource that supports transcoding Opus audio codec that is required for successful media negotiation. For more information, see the 'Opus Codec Transcoder Support' section in the "Configure Media Resource" chapter of the System Configuration Guide for Cisco 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 an 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.

Permanent License Reservation

Cisco Unified Communications Manager provides support for Permanent License Reservation that allows administrator to reserve an entitled Permanent License Tag from the Smart Account and Virtual Account against a Product instance. Administrators must provision the User Licenses as needed by the Product instance in the Smart Account and Virtual Account.

The feature is limited to FedRAMP customers. Permanent License Tag can be ordered through Cisco Commerce Workspace and is provisioned in the Smart Account and Virtual Account after Cisco's approval. For ordering, see the Cisco Collaboration Flex Plan 3.0 for FedRAMP Ordering Guide available at https://www.cisco.com/c/en/us/products/collateral/unified-communications/cisco-collaboration-flex-plan/guide-c07-744596.html.

Reserving Permanent License Tag prompts the administrator to specify the License count the system operates within. These can be referred on the License Management user interface and doesn't affect the compliance. The administrator must have those many User Licenses provisioned in the Smart Account and Virtual Account.

CLI Updates

The CLI commands available for License reservation can be used for reserving Permanent License Tag. The following new CLI command is introduced to support this feature:

- license smart reservation set license_count

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

Alarm and Alert Updates

Alert

The following alerts have been modified to support this feature:

- SmartLicense_Reservation_InEval
- SmartLicense_Reservation_NoProvision_EvalExpired
- SmartLicense_Reservation_ExportControlNotAllowed

For more details about these alerts, see the "Performance Counters and Alerts" chapter in the Cisco Unified Real-Time Monitoring Tool Administration Guide.

SSO Redirect URI for Webex Apps

The SSO Redirect URI feature allows soft clients (Cisco Jabber/Cisco Webex App) that use the external browser to perform SSO, be cross launched by the browser using SSO Redirect URI so that the browser can sign in to the Cisco Jabber/Cisco Webex App backend service.

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.

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.

Support for Download of Large Files from TFTP Server

Unified Communications Manager provides support for HTTP range requests (RFC7233) on the TFTP and Proxy TFTP (if the download file is at least 100MB). Endpoints that support HTTP range requests can benefit from improved reliability and download speed, especially in bulk phone upgrade scenarios or in poor network conditions.

HTTP range request support allows the downloads to pause and resume; meaning, interrupted downloads can continue from the last known successful byte-range without having to restart the entire download again.

At the time of release, the phone modes that support this feature are: Cisco Webex Wireless Phones 840 and 860.

For more information, see the 'Potential Issues with Firmware Installs' section in the "Manage Device Firmware" chapter of the Administration Guide for Cisco Unified Communications Manager.

Support for Meraki Access Points

Unified Communications Manager supports Location Awareness for wireless endpoints connecting through Meraki Access Points. For more information, see the chapter "Configure Location Awareness" in the Feature Configuration Guide for Cisco Unified Communications Manager.

Support for Secure Hash Algorithm (SHA-2)

The Unified Communications Manager now provides enhanced support to the SHA-2 algorithms on Skinny Client Control Protocol (SCCP) Gateway (Analog endpoints) and Hardware conference bridge (TLS and SRTP).

Note SHA-2 is not supported on the SCCP phones, H323, and MGCP.

For more information, see the 'SCCP Gateway and Hardware Conference Bridge Support for Secure Hash Algorithm (SHA-2)' section in the "Default Security" chapter of the Security Guide for Cisco Unified Communications Manager.

TFTP Proxy Support for OAuth

Unified Communications Manager now supports TFTP Proxy in SIP OAuth deployments. When SIP OAuth is enabled in TFTP Proxy setup, you must copy the Root CA certificate of off clusters Tomcat certificates to proxy phone edge trust.

Note Synergylite phone load version needs to be upgraded to 14.1. You must install this phone load to use this TFTP Proxy feature.

For more information, see:

- Enable SIP OAuth Mode section in the Feature Configuration Guide for Cisco Unified Communications Manager.
- Configure TFTP Server Manually and Configure TFTP Server Dynamically sections in the System Configuration Guide for Cisco Unified Communications Manager.

Wi-Fi to LTE Call Handoff

Wi-Fi to LTE Call Handoff provides flexibility for Cisco Webex users to switch between Wi-Fi and LTE networks without disconnecting any active calls that the user may be while switching network.

This feature is supported on both Cisco Webex Mobile and Desktop versions.

For more information, see the 'Wi-Fi to LTE Call Handoff' section in the Feature Configuration Guide for Cisco Unified Communications Manager.

Limit Persistent Chat Room Creation to Home Cluster

The IM and Presence Service is enhanced with the option to limit the creation of persistent chat rooms within Cisco Jabber user's home cluster by the IM and Presence Service administrator.

If Inter-clustering is enabled, this feature allows independent management of remote clusters without impacting accessibility of chat rooms to the users assigned to home cluster.

This feature reduces the inter-cluster traffic and increases the system bandwidth.

For configuration information, see the 'Limit Persistent Chat Room Creation to Home Cluster' section in the Configuration and Administration of the IM and Presence Service Guide.

Support for PostgreSQL 12.x

The IM and Presence Service further extends the support for PostgreSQL as an external data storage for compliance and persistent chat.

For configuration information, see the Database Setup Guide for the IM and Presence Service.

Shared Ownership of Persistent Chat Rooms

The IM and Presence Service supports administratively sharing the ownership of locally created chat rooms with any number of local room members.

This functionality is achieved by turning the existing **Room Report** into interactive user interface. As part of this feature, a new field **Owner ID** is introduced.

This feature allows transfer of room ownership from one owner to the other, and owner update in case of user ID change of the current owner.

For configuration information, see the 'Transferring Ownership of Persistent Chat Rooms' section in the Configuration and Administration of the IM and Presence Service Guide.

Important Notes

Simplifying Release Number Scheme

From Release 14 onwards, Cisco Unified Communications Manager has adopted the single number release plan. There will be no (dot) releases like (dot five) in the past release versions. Service Upgrade releases will be published on top of the main major release 14 through the regular Software Maintenance cycle.

New 2021 Signing Key

Attention The Release 14SU1 is signed with a new 2021 signing key. It is possible that you may need to install the ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn COP file first if upgrading from Unified Communications Manager versions prior to Release 14. See the COP file readme for specifics.

This release also removes support for the previous signing key. If you are installing phone firmware, ensure that you use the files with k4.cop.sha512 in the name, as these files are also signed with the new signing key. Installing files signed with the previous signing key results in a "The selected file is not valid." error during installation.

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 2: 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	11.5(1)SU10 and later	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

Gateway Model	11.5(x) Releases	12.5(x) Releases	14(x) Releases
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 3: 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

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 14SU1

You can search for defects in the Bug Search Tool at https://bst.cloudapps.cisco.com/bugsearch/.

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

- ReadMe for Cisco Unified Communications Manager, Release 14SU1
- ReadMe for Cisco Unified IM and Presence, Release 14SU1