Release Notes for Cisco Unified Communications Manager and the IM and Presence Service Release 14SU3

First Published: 2023-05-18

Last Modified: 2023-05-23

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:

- Unified Communications Manager: 14.0.1.13900-155
- IM and Presence Service: 14.0.1.13900-8

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 14.0.1.14[0-2]xx would be considered part of the 14SU3 (14.0.1.13900-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 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.

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

Auto Provision of Webex App and Cisco Jabber Devices

In Unified Communications Manager, you can auto provision the Webex App or Cisco Jabber devices when new LDAP users are synchronized from Microsoft Active Directory. The **Write back to LDAP** option allows you to write the Primary DN chosen from Unified CM back to the LDAP server. LDAP attributes available for write back are: telephoneNumber, ipPhone, and mobile.

User Interface Updates

To support this feature, the following menu items are updated in the Cisco Unified CM Administration user interface:

- In the **System > Service Parameters Configuration** page, a new service parameter **Provision Jabber Device As Part Of LDAP Sync** is added under "Cisco DirSync" service, to enable auto provisioning of Cisco Jabber devices.
- If the **Provision Jabber Device As Part Of LDAP Sync** service parameter is enabled and you have selected Microsoft Active Directory in the **System > LDAP > LDAP System Configuration** page, a new section **Jabber Endpoint Provisioning** is displayed on the LDAP Directory Settings page.

Centralized Call History

With this release, Webex Calling for Microsoft Teams users can view the call history for their shared devices which are registered to the Unified Communications Manager. For more information, see Webex Call Integration with Microsoft Teams for On-prem UCM.

To use this feature, the Unified Communications Manager node must be onboarded through Webex Cloud-Connected UC.

Microsoft Teams users must use Webex Calling integration for Microsoft Teams. For more information, see Webex Calling integration with Microsoft Teams.

Certificate Revocation List Support

Unified Communications Manager supports certificate revocation list, where the CA will have a list of digital certificates that have been revoked before their actual or assigned expiration date. To enable this feature you have to check the **Enable CRL** check box and enter the CRL Distribution Point URI from where the CRL files are downloaded.

For detailed information on the certificate revocation list support, see the 'Certificate Revocation Configuration' section in the Security Guide for Cisco Unified Communications Manager.

Cluster Software Location Updates

Unified Communications Manager now makes it easier to specify where cluster nodes will find their ISO files for upgrade or COP files, using the **Cluster Software Location** menu from the Cisco Unified OS Administration user interface.

In this release, you can centrally manage the Software Location settings for all cluster nodes from the publisher instead of locally on each cluster node.

User Interface Updates

To support the feature for this release, the following menu items are updated:

- You can add, edit, or modify any of the existing configurations for any node in the same cluster by navigating to the **Software Upgrades > Cluster Software Location** menu item in the Cisco Unified OS Administration user interface.
- Fields in the **Software Installation and Upgrade** menu item is now enabled for editing.

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

CLI Update

If you want to modify the existing Software Location configurations for any node in the same cluster, either use the CLI prompts on the local node or quit and login to use the **Software Upgrades > Cluster Software**

Location menu from the Cisco Unified OS Administration user interface of a Unified CM publisher. To install upgrades and COP files from both local and remote directories for a single node or cluster nodes, use the following commands:

- utils system upgrade
- utils system upgrade cluster

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

Device Mobility Support for Webex App on VDI

From Release 12.5(1)SU7a, Unified Communications Manager supports thin-client IPs to be used for device mobility instead of Hosted Virtual Desktop (HVD) IPs for Webex client. However, from Release 14SU3 onwards, the Cisco Unified CM Administration UI displays the HVD IP address, in addition to the thin-client IP address for the Webex Virtual Desktop Infrastructure (VDI) clients. This feature is supported from Webex App VDI version 43.2 onwards. The display of HVD IP address on the UI enables better serviceability and debugging.

UI Updates

To support this feature, the following menu item has been updated in the Cisco Unified CM Administration UI:

- In the **Device > Phone > Find and List Phones > Phone Configuration > Real-time Device Status** section, a new field **Hosted Virtual Desktop Address** is added.

Eliminate Refresh Token Dependency on Publisher for OAuth

OAuth feature is now enhanced to eliminate refresh token dependency on Unified Communications Manager publisher node by providing access to the subscriber node to update the refresh token.

For more information, see the 'System Parameters Task Flow' section of the "Configure Enterprise Parameters and Services" chapter in the System Configuration Guide for Cisco Unified Communications Manager.

iOS Local Push Connectivity for Calls

Webex App is not notified of incoming VoIP call notifications when an iOS device operates in a Wi-Fi constrained network with no internet connection such as, hospitals, cruise ships, airplanes, and so on. Due to lack of internet connectivity, the device does not have access to the Apple Push Notification Service (APNS). Users expect to receive calls without any delay. However, with APNS a call can be delayed for a few seconds when there is a network latency.

With this release, Local Push Notification Service (LPNS) for calls has been introduced for iOS devices. It helps to minimize any delay as the push message is sent to the client through a persistent connection. For more information, see the 'Local Push Notification Service' section in the Push Notifications Deployment Guide.

To know the minimum required iOS version for Webex App, see System requirements for Webex services.

Managed File Transfer Enhancements

The IM and Presence Service is enhanced to support OpenSSH 8.x and extends the public key length support to 4096 bits, for establishing connections with the External File Server.

For configuration information, see the "Configure Managed File Transfer" chapter in the Configuration and Administration of the IM and Presence Service Guide.

SRTP DTMF Interworking

Currently, Unified Communications Manager inserts MTP for a DTMF mismatch in both secure and non-secure calls. But for secure calls, though MTP is inserted for a DTMF mismatch, it just passes through the media between the parties. Hence, the DTMF events are not sent between the parties. Before Unified CM Release 14SU3, DTMF translation worked only for non-secure calls when there was an MTP allocated for a DTMF mismatch.

With this release, Unified CM can invoke a hardware MTP (with SRTP DTMF interwork support) for a DTMF mismatch between secure endpoints. For more information, see the 'SRTP DTMF Interworking' section in the "Configure Media Resource" chapter of the System Configuration Guide for Cisco Unified Communications Manager.

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 Update releases will be published on top of the main major release 14 through the regular Software Maintenance cycle.

SIP Secure Phone Registration

From this release onwards, memory usage increases for SIP secure phone registrations although it does not impact the server capacity in most of the deployments.

New 2021 Signing Key

Attention Release 14SU1 and onwards 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	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 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 14SU3

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 14SU3
- ReadMe for Cisco Unified IM and Presence, Release 14SU3