Release Notes for Cisco Unified Communications Manager Release 14SU2 and the IM and Presence Service Release 14SU2a

First Published: 2022-06-15

Last Modified: 2022-07-05

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 Release 14SU2: 14.0.1.12900-161
- IM and Presence Service Release 14SU2a: 14.0.1.12901-1

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

Borderless Computer Telephony Integration (CTI) Protocol

In the existing Unified Communications Manager, CTI applications had to have a direct TCP connection to CTI Manager to leverage CTI control. As a result, Webex Apps could not be used in Desk Phone Control Mode or Extend and Connect Mode when the client was off-premises.

With this release, Webex App supports Desk Phone Control Mode/Extend and Connect Mode for clients connecting remotely. To use this feature, the Unified Communications Manager node must be onboarded through Cloud-Connected UC.

Cluster Software Location

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.

You can:

- Add, edit, or modify any of the existing configurations for any node in the same cluster from the Unified Communications Manager publisher as a one-stop shop.

- Apply the same software location details to all the other nodes in the cluster, including the publisher.

User Interface Updates

To support this feature, the following menu item is added on the Unified Communications Manager publisher:

- In the Software Upgrade page of the Cisco Unified OS Administration user interface, the **Cluster Software Location** menu item is added.
- Fields in the **Software Installation and Upgrade** and **Software Installation and Upgrade Cluster** menu items are now disabled and are read-only information. You can add, edit, or modify any of the existing configurations of a node by selecting the **Software Upgrades > Cluster Software Location** menu in the Cisco Unified OS Administration user interface.

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

CLI Update

In Release 14SU2, Software Location settings for all cluster nodes are centrally managed from the Publisher instead of locally on each cluster node. If you want to add, edit, or modify any of the existing configurations for any node in the same cluster, navigate to the **Software Upgrades > Cluster Software Location** menu from the Cisco Unified OS Administration user interface before you begin to upgrade your system. 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.

Emergency Calling for National Suicide Prevention Lifeline

Unified Communications Manager supports dialing '988' calls, that are 3-digit dialing codes that will be routed to the National Suicide Prevention Lifeline centers. All telecommunication carriers and interconnected voice over Internet Protocol (VoIP) service providers will offer this service to connect with suicide prevention and mental health crisis personnel. This is in support of the FCC mandate of supporting a 3-digit dial code for Suicide Prevention Hotline that comes into effect from July 22, 2022.

For more information, see: https://www.fcc.gov/suicide-prevention-hotline.

External Phone Number Mask

In Unified Communications Manager, the External Phone Number can be masked for all configured line numbers for the latest phone models. Existing phone models continue to display the External Phone Number Mask for the primary line.

Note The supported phone models are 78xx and 88xx series.

Inclusion of Organisation Unit field

From Unified Communication Manager 14 SU2 release onwards, the Organization Unit field is removed by default from the Certificate Signing request. From this release onwards you can choose **Include OU** in CSR option to include the Organization Unit field in the Certificate Signing Request.

For more information, see the section 'Self-Signed Certificate Fields' of the Security Guide for Cisco Unified Communications Manager

LSC Certificate Enrollment using EST

Unified Communications Manager now includes Certificate Authority Proxy Function (CAPF) Online CA type “EST Supported CA” to support the automatic enrollment of certificates with CAs having inbuilt EST server mode.

User Interface Updates

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

- In the **System** > **Service Parameters** > **Service Parameter Configuration** > **Online CA Parameters** section:
    - New drop-down option for Online CA Type field—EST Supported CA
    - New field—Certificate Enrollment Profile Label

RedSky E911 Location Services Support

The RedSky solutions integrated with Unified Communications Manager allow the clients to have an active location URI for 9-1-1 emergency calling coverage for their entire workforce, whether on campus or remote, and send the calls to emergency responders. For more information, see the "Emergency Call Handling with RedSky" chapter in the Feature Configuration Guide for Cisco Unified Communications Manager.

Secure Call Support for Parking Lot

In the existing Unified Communications Manager, when a secure call is placed to a Hunt Pilot and all the Line Groups are busy, the call is temporarily placed on hold. If the endpoint does not support Secure Real-Time Transport Protocol (SRTP) fallback, the call that is placed to Parking Lot (non-secure device) drops off due to crypto mismatch.

With this feature, the Unified CM handles the originating SRTP-only call as a secure call throughout, irrespective of the SRTP fallback option status. For more information, see the 'Secure Call Queuing' section in the "Configure Call Queuing" chapter of the Feature Configuration Guide for Cisco Unified Communications Manager.

SRTP Cipher Mismatch with Media Streaming Devices

Unified Communications Manager now supports all crypto ciphers while exchanging call capabilities post Cisco IP Voice Media Streaming (IPVMS) devices (MOH, IVR, or Annunciator) after mid-call events, such as transfer or hold, from the remote side. With this feature, the current active secure calls or security is not impacted. For more information, see the 'SRTP Cipher Mismatch with Media Streaming Devices' section in the "Default Security" chapter of the Security Guide for Cisco Unified Communications Manager.

Unified Communications Manager and IM and Presence Service Cluster Upgrade Limitation from Older Versions

Unified Communications Manager's FIPS Mode constraints have now been upgraded (CiscoSSL, CiscoFOM, and CiscoSSH to 7. X) and that limits the use of the SSH-RSA algorithm in the FIPS mode. The older version of Unified CM uses OpenSSH 5. X which does not support the latest SSH algorithms. You must deploy the COP files before upgrading the clusters in FIPS mode. If you are upgrading any of your older Unified CM or IM and Presence Service versions to Release 14SU2 in FIPS mode, install the COP file *ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop*.

For more information, see the 'Supported Upgrade and Migration Paths with COP Files' section in the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service.

If your 14SU2 version of Cisco Prime Collaboration Deployment is in FIPS mode and you are using any of the Pre-12.5 UC clusters to perform cluster discovery, upgrade, or migration, you must first switch your Cisco Prime Collaboration Deployment to work in the non-FIPS mode before proceeding with any of these tasks. For Direct Standard Upgrade or Migration of UC clusters in FIPS mode with the Pre-14SU2 releases, install the COP file *ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop* on the UC clusters.

For more information, see the 'Supported Tasks for Applications and Versions' section in the Prime Collaboration Deployment Administration Guide, Release 14.

Windows Authentication for MSSQL Database for Persistent Chat

The IM and Presence Service supports Windows authentication for MSSQL external database.

When this feature is enabled, Windows groups can be created at the domain level and a login can be created on MSSQL Server for the entire group. For more information, see the 'Windows Authentication for MSSQL Database for Persistent Chat' 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 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	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
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 Unified CM 14SU2 and IM and Presence Service 14SU2a

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 14SU2
- ReadMe for Cisco Unified IM and Presence, Release 14SU2a