Important Notes

Blue Screen Appears for Unified CM Refresh Upgrades

An issue exists with refresh upgrades of Unified Communications Manager to specific destination releases. After the timezone data populates, you may see a blue transition screen appear for 30 minutes or more.

If you see this blue screen, DO NOT stop the upgrade, or a kernel panic occurs. The upgrade will continue to run even while the blue screen displays. The blue screen will clear itself after approximately 30 minutes

Affected 'To' Versions

This issue affects refresh upgrades of Unified Communications Manager where the destination version falls within the range in the below table. This range includes SU and ES versions that lay within the range. This issue does not occur for upgrades to older or newer versions that do not fall within the range, or for upgrades of the IM and Presence Service.

Table 1: Affected 'To' Versions for Blue Screen Refresh Upgrade Issue

Release Category	Affected Upgrade Destination Range
10.5(x)	10.5.2.21170-1—10.5.2.22188-1 (includes 10.5(2)SU9)
11.5(x)	11.5.1.16099—11.5.1.17118-1 (includes 11.5(1)SU6)
12.0(x)	12.0.1.23036-1 — 12.0.1.24053-1 (includes 12.0(1)SU3)

Release Category	Affected Upgrade Destination Range
12.5(x)	12.5.1.11001-1 — 12.5.1.12018-1 (includes 12.5(1)SU1)

For additional details, see CSCvs28202.

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 (e.g., 10.5(2), 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 2: 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

Gateway Model	10.5(2) Releases	11.5(x) Releases	12.0(x) Releases	12.5(x) Releases	14(x) Releases
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	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 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	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.

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 4: 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	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).

Scenario	Procedure

Upgrade from IM and Presence 11.5(1)SU3 or later	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)..
	
	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 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.)

Video Endpoint Migration Requirements

If you are migrating Cisco TelePresence endpoints to any Cisco Unified Communications Manager 12.x release, it's highly recommended that you upgrade firmware to CE 9.8 or later before you migrate. Otherwise, Unified CM overwrites the existing endpoint configuration with default settings during device registration. This issue occurs because CE 9.7 and earlier does not have any method to communicate the existing configuration to Unified CM. If the endpoint is running CE 9.8 or higher, the endpoint sends the existing configuration to Unified Communications Manger during registration, thereby letting the administrator provision settings.

If you are registering existing TelePresence endpoints to a new Unified CM cluster, and maintaining the endpoint settings is required, make sure to use **Endpoint Configuration Mode** on Unified CM. Otherwise, Unfiied CM pushes its settings out to the endpoint. After you complete registration, you can change the configuration mode to whatever mode you want.

For procedures on how to migrate existing TelePresence endpoints to Cisco Unified Communications Manager, refer to the "Video Endpoints Management" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU1*.

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).