New and Changed Features

AES 80-Bit Authentication Support

Cisco Unified Communications Manager supports Advanced Encryption Standard (AES) with a 128-bit encryption key and a 32-bit authentication tag used as the encryption cipher. With this release, the AES 32-bit authentication tag is enhanced to an 80-bit authentication tag used as the encryption cipher on Music On Hold (MOH), Interactive Voice Response (IVR), and Annunciator. This enhancement helps customers using 80-bit authentication tag to make the Secure Real-Time Transport Protocol (SRTP) calls over a SIP line and SIP trunk.

For more information, see the Encrypted Phone Configuration File Setup chapter in the *Security Guide for Cisco Unified Communications Manager*.

Audit Logging for Disabled Inactive User Accounts

With this release, the Cisco Database Layer Monitor disables inactive users and then audit logs the same.

Cisco Database Layer Monitor changes the user account status to inactive during scheduled maintenance tasks if you have not logged in to Unified Communications Manager within a specified number of days. The disabled user details are audited automatically and the audit log displays the message as: “<`userID`> user is marked inactive”.

For more details on how to Disable Inactive User Accounts, see the “Manage User Access” chapter of the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Authenticated Network Time Protocol Support

With this release, Unified Communications Manager supports Network Time Protocol (NTP) authentication through the Autokey protocol, which uses a combination of Public Key Infrastructure (PKI)-based authentication and a pseudo-random hash sequence. Previously, NTP authentication was provided through the symmetric key only. With this update, you can authenticate NTP messages with either method.

This feature enhances the security of your system by providing encrypted PKI-based protection for the NTP messages on your network. Authenticated NTP through autokey helps your system to comply with Common Criteria Guidelines as PKI-based authentication is mandatory for Common Criteria compliance.

To enable this feature, NTPv4 must be running with Red Hat Package Manager (rpm) version ntp-4.2.6p5-1.el6.x86_64.rpm and above.

Choosing an NTP Authentication Method

When choosing which NTP authentication method to deploy, consider the following:

- RedHat recommends the symmetric key over autokey. For more information, see https://access.redhat.com/support/cases/#/case/list.
- Common Criteria compliance mandates that you use a public key.

Configuration

Configure NTP on the publisher node only as Cisco Unified Communications Manager synchronizes the NTP time of all subscribers in the cluster to the publisher automatically. For more information on how to configure NTP and NTP authentication, see the “Configure NTP” chapter in the *System Configuration Guide for Cisco Unified Communications Manager*.

Note To configure NTP authentication through autokey, you must first enable Common Criteria mode in your system. For details on Common Criteria mode, see the “FIPS Setup” chapter of the *Security Guide for Cisco Unified Communications Manager*.

CLI Reference Guide Updates

To support this feature, the **utils ntp auth auto-key {enable| disable| status}** has been added. For CLI details, refer to the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

BE6000 Licensing Support

Smart Licensing: BE6000 Licensing Support

A new command **utils BE6000Mode** is added in the Unified Communications Manager and IM and Presence Command Line Interface.

Unified Communications Manager 12.5(1) in a Business Edition 6000 solution requires BE6000 Mode to use Business Edition 6000 starter pack licenses.

The following options are added with the new command:

- utils BE6000Mode- With this option, you can enable BE6000 Mode on Unified Communications Manager.
- utils BE6000Mode disable- With this option, you can disable BE6000 mode on Unified Communications Manager.
- utils BE6000Mode status- With this option, you can view the status of the BE6000 mode on Unified Communications Manager.

For more information on CLI, see the "utils BE6000Mode" section of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* guide at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Call Management Records for SIP Trunk

In previous releases, Unified Communications Manager generated Call Management Records (CMRs) that included call quality metrics for SIP phones. With this release, Unified Communications Manager generated CMRs include call quality metrics for SIP trunk calls through a Cisco Unified Border Element (CUBE) or IOS gateways. This update helps customers to evaluate the voice quality metrics for SIP trunk calls.

CUBE sends the call statistics in a P-RTP-Stat header in a BYE message or a 200 OK response to BYE message to update the CMRs in Unified Communications Manager. Call statistics include Real-time Transport Protocol (RTP) packets sent or received, total bytes sent or received, total number of packets that are lost, delay jitter, round-trip delay, and call duration.

Prerequisites for Reporting Call Statistics in CMRs for SIP Trunk

- Cisco IOS Release 15.1(3)T or a later release must be installed and running on your Cisco Unified Border Element.
- Cisco IOS XE Release 3.3S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

For more information, see the "Call Management Records" chapter in the *Call Detail Records Administration Guide for Cisco Unified Communications Manager*.

Call Recording for SIP or TLS Authenticated Calls

Prior to 12.5(1) version, the phones which are authenticated (phone with Security profile having Device Security Mode as Authenticated) were not allowed to make use of the Call Recording feature. Whereas, Non–Secured phones or Secured/ Encrypted phones could use Call Recording feature with Non-Secured or Secured recorders, respectively. With the release 12.5(1), Cisco Unified CM JTAPI interface has been enhanced to allow recording in Authenticated Phones based on the value of the new service parameter **Authenticated Phone Recording**.

The expectation is that the authenticated phones should also be allowed to make use of the Call Recording feature. It depends on value set in the newly added service parameter **Authenticated Phone Recording** which can be set to the following values:

- **Allow Recording** – Authenticated Phones can be allowed to record the calls.
- **Do Not Allow Recording** – Authenticated Phones cannot make use of Call Recording feature. This is the default value for the service parameter. The behavior would be the same as that of the current behavior.

Backward Compatibility

This feature is backward compatible. JTAPI will support the current API's.

Security Update to Cisco JTAPI Client

With this release, Cisco JTAPI Client for Linux (32 and 64 bit) plugin uses Cisco security providers instead of RSA security providers.

Cisco JTAPI Package Download Details

With this release, the JTAPI installation files for Windows and Linux are provided through zip files. The zip files, which are accessible on the **Application** > **Plugins** page in Cisco Unified CM Administration, must be unzipped before installing JTAPI.

The zip packages include:

- JTAPI packages for Linux (32 and 64 bit) or Windows (32 and 64 bit)
- Documentation
- Sample codes

The CiscoJ Libraries of Linux (32 and 64 bit) can be downloaded from the plugins URL:

- https://<*IP address*>/plugins/lib_ciscoj_x32.zip
- https://<*IP address*>/plugins/lib_ciscoj_x64.zip

The zip file (CiscoJTAPIWindows.zip and CiscoJTAPILinux.zip) replaces the following installers:

- CiscoJTAPIClient-linux.bin
- CiscoJTAPIClient.exe
- CiscoJTAPIx64-Windows.exe
- CiscoJTAPIx64-Linux.bin

Note For more information on CLASSPATH and LD_LIBRARY_PATH, see the readme file, which is part of the zip file.

User Interface Updates for Cisco JTAPI Client

The following changes have been made in the **Find and List Plugins** window (**Application** > **Plugins**).

- The **Cisco JTAPI 32-bit Client for Linux** and **Cisco JTAPI 64-bit Client for Linux** links under the **Plugin Name** column is changed to **Cisco JTAPI Client for Linux-32-bit and 64-bit**.
- The **Cisco JTAPI 32-bit Client for Windows** and **Cisco JTAPI 64-bit Client for Windows** links under the **Plugin Name** column is changed to **Cisco JTAPI Client for Windows-32-bit and 64-bit**.

The **Description** column details are updated. For more details, see the Cisco Unified CM Administration interface.

For more details on installation, see the “Cisco Unified JTAPI Installation” chapter of the *Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager, Release 12.5(1)*, at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html.

Cisco JTAPI Support for RHEL 7

With this release, Cisco JTAPI supports RHEL 7 for 64 bit on the Linux operating system. Previously, it supported RHEL 6.

Support for VMware

Cisco JTAPI is used on VMware ESXi version 4.0. The application uses Windows 2003 and Windows 2008 virtual machines on the VMware version to run Cisco JTAPI. For more information on the supported Java Virtual Machines, see the following table:

Table 1: Supported JVM Versions for Unified Communications Manager

Operating System	Version	Unified CM 10.0	Unified CM 10.5	Unified CM 11.0	Unified CM 11.5	Unified CM 12.0	Unified CM 12.5
Linux	AS 3.0	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported
Linux	RHEL 7 (64 bit)	Not supported	Not supported	Not supported	Not supported	Not supported	Supported
Linux	RHEL 3.7	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported
Linux	RHEL (32 bit)	RH 5.5 Sun JVM 1.6.0.29	RH 5.5 Oracle JVM 1.7.0.40	RH 5.5 Oracle JVM 1.7.0.76	RH 5.5 Oracle JVM 1.7.0.79	RH 5.5 Oracle JVM 1.7.0.79	RH 5.5 Oracle JVM 1.7.0.79
Linux	RHEL 5.5 (64 bit)	Sun JVM 1.6.0.29	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79
Linux	RHEL 6 (64 bit)	Sun JVM 1.7.0.40	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79
Solaris	6.2 on Sparc and x86	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported
Windows	Windows XP 2003, 2008 Server(32-bit)	Sun JVM 1.6.0.29	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Not supported	Not supported
Windows	Vista (32 bit)	Sun JVM 1.6.0.29	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Not supported	Not supported
Windows	Windows 7(32 and 64 bit) 2008 Server R2(64 bit)	Sun JVM 1.6.0.29	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79
Windows	Windows 8(32 and 64 bit)	Sun JVM 1.6.0.29	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79
Windows	Windows Server 2012 R1 (32 bit)	Sun JVM 1.6.0.29	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79

Operating System	Version	Unified CM 10.0	Unified CM 10.5	Unified CM 11.0	Unified CM 11.5	Unified CM 12.0	Unified CM 12.5
Windows	Windows 8.1(32 and 64 bit)	Not supported	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79
Windows	Windows Server 2012 R2 (64 bit)	Sun JVM 1.7.40	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79
Windows	Windows 10(32 and 64 bit)	Not supported	Oracle JVM 1.7.0.40	Oracle JVM 1.7.0.76	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79
Windows	Windows Server 2016(64 bit)	Not supported	Not supported	Not supported	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79	Oracle JVM 1.7.0.79

For more details on Cisco Unified JTAPI, see “Features Supported by Cisco Unified JTAPI” chapter in the *Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html.

CiscoSSH Support with FIPS Mode

Cisco Unified Communications Manager now uses CiscoSSH instead of OpenSSH. When you enable FIPS mode on your system, CiscoSSH also switches to FIPS mode automatically.

For details on how to enable FIPS mode, see the "FIPS 140-2 Setup" chapter of the Security Guide for Cisco Unified Communications Manager.

CiscoSSH Support

CiscoSSH supports the following key exchange algorithms:

- **Diffie-Hellman-Group14-SHA1**
- **Diffie-Hellman-Group-Exchange-SHA256**
- **Diffie-Hellman-Group-Exchange-SHA1**

CiscoSSH supports the following ciphers with the Unified Communications Manager server:

- **AES-128-CTR**
- **AES-192-CTR**
- **AES-256-CTR**
- **AES-128-GCM@openssh.com**
- **AES-256-GCM@openssh.com**

- **AES-128-CBC** (supported for Release 12.0(1) and up)
- **AES-192-CBC** (supported for Release 12.0(1) and up)
- **AES-256-CBC** (supported for Release 12.0(1) and up)

CiscoSSH supports the following ciphers for clients:

- **AES-128-CTR**
- **AES-192-CTR**
- **AES-256-CTR**
- **AES-128-GCM@openssh.com**
- **AES-256-GCM@openssh.com**
- **AES-128-CBC**
- **AES-192-CBC**
- **AES-256-CBC**

Cipher Management

The cipher management feature enhances the security of your system by allowing you to disable weak ciphers on different secure interfaces on Cisco Unified Communications Manager and IM and Presence. Cipher management allows you to control the set of security ciphers that is allowed for every TLS and SSH connection.

This feature allows you to configure the recommended ciphers without breaking the compatibility with other components such as older model phones, or any entity that is securely connected to Cisco Unified Communications Manager and IM and Presence.

For more information, see the "Cipher Management" section in the *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

User Interface Updates

The **Cipher Management** window is added to the **Security** menu of the Cisco Unified OS Administration and Cisco Unified IM and Presence OS Administration interfaces.

For more information, see the "About Cipher Management" section in the *Cisco Unified Operating System Administration Online Help*.

For more information on the **Curve Negotiation** and **Supported Ciphers for EC Curves**, see the "Curve Negotiation" section in the *Security Guide for Cisco Unified Communications Manager, Release 12.5(1)*.

Configure Maximum Login Time for Extension Mobility and Extension Mobility Cross Cluster

With this release, you can configure the maximum login time for Extension Mobility and Extension Mobility Cross Cluster at the user level. If you have configured the user profile configuration page to permit it, your users can also set the maximum login time through the Cisco Unified Communications Self-Care Portal.

You can also add or update the maximum login time for a group of users through Bulk Administration.

For the Extension Mobility service parameter, you can now set the value of **Intra-cluster Maximum Login Time** to zero, rather than changing the value of **Enforce Intra-cluster Maximum Login Time** to False.

User Interface Updates

- In Cisco Unified CM Administration, the **Maximum Login Time (HHH:MM)** parameter is added on the **End User Configuration** page under the **User Management** > **End User**.
- In Cisco Unified CM Administration, the **Allow End User to set their Extension Mobility maximum login time** checkbox is added on the **User Profile Configuration** page under the **User Management** > **User Settings** > **User Profiles**.
- In Cisco Unified Communications Self-Care Portal, the following radio buttons are added under **General Settings** > **Extension Mobility**:
  - Use system default Maximum Login Time
  - No Maximum Login Time
  - Automatically log me out after hours___minutes___
- In Cisco Unified CM Administration, the **Maximum Login Time (HHH:MM)** parameter is added on the **User Template Configuration** page under **Bulk Administration** > **Users** > **User Template**.
- In Cisco Unified CM Administration, the **Maximum Login Time (HHH:MM)** parameter is added on the **Update Users Configuration** page under **Bulk Administration** > **Users** > **Update Users** > **Query**.
- In Cisco Unified CM Administration, the **EM MAX LOGIN TIME** field is added in the BAT Spreadsheet under **Bulk Administration** > **Upload/Download Files**.
- In Cisco Unified CM Administration, the **EM MAX LOGIN TIME** field is added in the View Sample File under **Bulk Administration** > **Users** > **Insert Users**, **Bulk Administration** > **Users** > **Update Users** > **Custom File**, and **Bulk Administration** > **Phones & Users** > **Insert Phones with Users**.

For more information on configuring maximum login time for Extension Mobility, see the following:

- "Configure User Profiles" section of the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
- "Set the Maximum Login Time for Extension Mobility" section of the *Cisco Unified Communications Self Care Portal User Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-user-guide-list.html.

For more information on configuring maximum login time for Extension Mobility for bulk users, see the *Bulk Administration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

For more information on Extension Mobility service parameters, see the "Extension Mobility Service Parameters" section of the *Feature Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Encrypted IM Compliance Database

This release of the IM and Presence Service supports an encrypted compliance database for the Message Archiver feature. When this feature is deployed, all instant messages are encrypted before they get sent to the compliance database. Anyone looking at the data within the compliance database is unable to read the archived messages without an encryption key.

This feature provides greater security for your IM and Presence deployment by allowing your system to comply with compliance regulations, while restricting read access for potentially confidential IM exchanges to authorized personnel. For example, let’s say that your company uses instant messaging to communicate with customers, and your company does business in a regulated industry that requires message archiving. By restricting access to the encryption key, you can archive all instant messages, provide employees such as a database administrator with the database access that they need to keep the system running, while still limiting read access to archived IM exchanges to only those employees with a genuine business need.

This feature is supported only if you have Microsoft SQL Server deployed as the external compliance database.

Intercluster Networks

For intercluster networks, you can enable encryption for the intercluster network from a single cluster, which then becomes the master cluster for the network. The master cluster syncs its encryption key and encryption settings to the remote clusters, which become the slave clusters in the intercluster network. Encryption is configured automatically for remote clusters, provided the Message Archiver feature is configured in the remote cluster, with a Microsoft SQL Server compliance database.

Encryption Standards

To ensure that archived data is not compromised, this feature uses three keys: a symmetric encryption key, along with an assymetric public-private key pair.

- Encryption key—This 256-bit symmetric key is generated and stored internally by the IM and Presence Service, which uses this key to encrypt IM compliance data before archiving the data in the compliance database. For intercluster networks, the master cluster syncs its encryption key to the remote slave clusters so that the entire intercluster network is using the same encryption key, which is controlled from the master cluster.

  You must download this key from the IM and Presence Service and use it with your data viewer to be able to decrypt archived IMs. When you download this key, the key is encrypted with the public key from the public-private key pair. You can later decrypt the encryption key with the private key.

- Public-Private key pair—You must generate this assymetric key pair in an approved key generation tool (for example, OpenSSL) and use it to encrypt the key in the IM and Presence Service and then decrypt the key with your data viewing tool. The public-private key pair secures the encryption key while in transit from the IM and Presence Service to your data viewing tool (for example, Splunk).

The encryption password is hashed with SHA2 and then encrypted with AES 256. Instant Messages are encrypted with the AES 256 algorithm

Process Flow for Encryption

The following table highlights the process flow for enabling encryption and for viewing encrypted data from the database. The flow highlights each step, and the interface on which each step is completed.

Table 2: Encryption Process Flow

	IM and Presence Service Master Cluster	Key Generation Tool (e.g., OpenSSL)	Data Viewing Tool
Step 1	The administrator configures encryption for the intercluster network. The master cluster syncs encryption settings across the intercluster network. Archived data is now encrypted.	—	—
Step 2	—	The administrator generates a public-private key pair for securing the encryption key.	—
Step 3	The administrator downloads the encryption key from the IM and Presence Service. During the download, the public key encrypts the encryption key.	—	—
Step 4	—	—	The administrator uses the private key to decrypt the encryption key.
Step 5	—	—	The encryption key decrypts compliance data. Authorized personnel can view archived compliance data.

Minimum Requirements

The following requirements apply for this feature

Table 3: Minimum Requirements for Encrypted IM Compliance Database

System	Requirements for this Feature
IM and Presence Service	• For 11.x releases, the minimum release for this feature is 11.5(1)SU5. • For 12.x releases, the minimum release will be 12.5(1). • This feature is not supported with 12.0(1) or 12.0(1)SU1. If you have this feature deployed in 11.5(1)SU5 and you upgrade to 12.0(1) or 12.0(1)SU1, you will lose this feature.
External Database	• You must have Microsoft SQL Server deployed as your compliance database on all cluster nodes to support this feature.

Configuration

For details on how to configure an encrypted database for the Message Archiver, refer to the "Message Archiver Configuration" chapter of the *Instant Messaging Compliance Guide for the IM and Presence Service.*

User Interface Updates

To support this feature, the **Encryption settings for external database** section has been added to the **Compliance Settings Configuration** window. This set of fields appears only if you configure the **Message Archiver** and select a Microsoft SQL Server compliance database. This section contains the following fields, all of which are added for this release:

- **Enable Encryption on this cluster**—Check this check box to enable encryption in the local cluster
- **Enable Encryption on Remote Clusters**—Check this check box to enable encryption on intercluster peers in an intercluster network. The local cluster becomes the master cluster, which syncs its encryption key to the remote clusters, which are slave clusters.
- **Password/Confirm Password**—Enter the encryption password. You will need to reenter this password if you want to download the encryption key, disable encryption, or change the encryption password.
- **Status table for this cluster**—This read-only status table displays the status of any intercluster syncs, and which also displays which cluster is the master cluster. The table displays the following status columns:
    - Successful Modification Date—The result of the last successful configuration modification for both encryption passwords, and encryption status.
    - Failed Modification Date—If any attempts to change the encryption password or encryption status failed, the results display here.
    - Master Cluster ID—This field identifies which cluster, in an intercluster peer setup, is the master cluster.
- **Change Password**—If encryption is configured, click this button to change the password. You can only change the password on the master cluster.

- **Download Encryption Key**—Click this button to download the encryption key. To download the key, you must enter the encryption password as well as the public key that you generated with the external Windows tool.
- **Disable Encryption**—Check this check box to disable encryption.

Alarm Updates

The **MAencryptionMultiMaster** alarm has been added under the Cisco XCP Message Archiver service to indicate an issue with message archiver encryption. This alarm will be raised whenever you have an intercluster peer network where more than one cluster is configured as a master cluster for message archiver encryption.

Elliptical Curve Cryptography For On Premise Calls

Cisco Unified Communications Manager support Elliptical Curve Cryptography for point-to-point calls between supported Cisco IP phones.

Elliptical curve cryptography provides comparable security to a 3072-bit RSA public key while using smaller keys. This eases your data storage and data transmission requirements while maintaining a high level of system security.

This feature is supported for on premise calls only, and is not supported for Mobile and Remote Access deployments. To use Elliptical Curve Cryptography, your system and devices must all support elliptical curves.

Configuration

To configure the system to use elliptical curves, you must make sure that the Cipher Management interface allows ciphers that use elliptical curves. For details on how to use Cipher Management window to configure system ciphers, refer to *Security Guide for Cisco Unified Communications Manager, Release 12.5(1)*.

Enhancement to Universal Device or Line Template

With this release, Universal Device Template and Universal Line Template functionalities are enhanced to make the device provisioning easier.

This feature provides the following enhancements:

- Add a new phone with or without a user- You can add a new phone using the Universal Device Template with or without associating to a user. For example, conference room phone or lobby phone. See the "Add New Phone from Template with or Without an End User" section in the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service* at the http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
- Copy the Universal Device Template or Universal Line Template- You can create a new Universal Device Template or Universal Line Template by copying the existing templates and making required minor modifications. See the "Configure Universal Line Template" and the "Configure Universal Device Template" sections in the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service* at the http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

- Import or Export of Universal Device Template and Universal Line Template- The Bulk Administration Tool (BAT) supports Import or Export of Universal Device Template and Universal Line Template. You can export the existing Universal Device Template or Universal Line Template and make minor site-specific modifications and import. See "Export Configuration Data Options" section in the *Bulk Administration Guide for Cisco Unified Communications Manager* at the http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
- Non-Size Safe Phone Button Layouts- You can create an individual phone button template or use the phone button template from device defaults by setting the Phone Template Selection for Non-Size Safe Phone and Auto Registration Legacy Mode enterprise parameter on **Enterprise Parameters Configuration** page. This feature reduces unnecessary Phone Button template creation. See "Phone Button Template" section in the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service* at the http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
- TAG or Token- You can configure more parameters as TAG or token for Universal Device Template.

User Interface

- To add a new phone with or without a user, **Add New From Template** button is added under the **Device** > **Phone** > **Find and List Phones** menu of the Cisco Unified CM Administration interface.
- To Import or Export Universal Device Template and Universal Line Template, Universal Device Template and Universal Line Template parameters are added under the **Bulk Administration** > **Import/Export** > **Export** > **User Data** .
- For Non-Size Safe Phone Button Layouts, the **Phone Template Selection for Non-Size Safe Phone** enterprise parameter is added on the **Enterprise Parameters Configuration** page.
- To copy the Universal Device Template and Universal Line Template, **Copy** button is added under the **Find and List Universal Device Templates** page, **Universal Device Template Configuration** page, **Find and List Universal Line Templates** page, and **Universal Line Template Configuration** page.
- Device Name #DEV#, Product Type #PDT#, Protocol Type #PROTO#, and Extension #EXT# tags are added in the **Build Input For Device Description** pop-up on the **Universal Device Template Configuration** page.
- Extension#EXT# and Line Index #LI# tags are added in **Build Input For Line label** pop-up on the **Universal Device Template Configuration** page.

Enhanced CLI Updates for Smart Licensing

You can now use the following CLI commands to choose how which Unified Communications Manager connects to the Smart Software Licensing service. The Direct option is selected by default where the product communicates directly with Cisco licensing servers.

- license smart transport direct
- license smart transport gateway <URL>
- license smart transport proxy <proxy-server> <proxy-port>

For more details about these CLI commands, see the License Commands" of the Command Line Interface Reference Guide for Cisco Unified Communications Solutions at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

FIPS Mode Mandates SHA256 Hash Algorithm

With this release, when your system is running in FIPS mode, certificates must be encrypted using the SHA256 hashing algorithm. If FIPS mode is enabled, when you generate a self-signed certificate or if you generate a Certificate Signing Request (CSR), the system gives you the option of using SHA256 as the hashing algorithm. You will not be able to select SHA1. With this enhancement, Cisco Unified Communications Manager is compliant with FIPS.

If you upgrade from an earlier release with FIPS mode enabled, any existing certificates that used SHA1 have regenerated automatically with SHA256 as the hashing algorithm.

For more details on FIPS mode, see the "FIPS Mode Setup" chapter in the *Security Guide for Cisco Unified Communications Manager*.

User Interface Updates

If FIPS mode is enabled, the **Hash Algorithm** drop-down that appears in the **Generate New Self-Signed Certificate** and **Generate Certificate Signing Request** dialog box, allows you to only select **SHA256**. However, if FIPS mode is disabled, you will still be able to select **SHA1** or **SHA256**.

Online Help Updates

The "Self-signed Certificate Fields" and "Certificate Signing Request Fields" tables now show that SHA256 is the hashing algorithm for Self-Signed Certificate and Certificate Signing Request by default.

For detailed help content with the fields, see the *Cisco Unified Administration CM Administration Online Help*.

Granular Access Control

Granular Access Control allows you to access the system while restricting access to tasks such as:

- Adding users
- Editing passwords
- Editing user rank
- Editing access control groups

For more details, see https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1/admin/cucm_b_administration-guide-1251/cucm_b_administration-guide-1251_chapter_010.html.

Intercluster Peer Sync Enhancements

This release of the IM and Presence Service includes enhancements to the Cisco Intercluster Sync Agent to make it easier to resolve syncing issues when intercluster peers are unable to sync. By default, your system now monitors intercluster peer sync statuses. If any peer cluster syncing issues are found, Cisco Intercluster SyncAgent automatically restarts to resolve the issue. This ensures that your intercluster network connections remain up and running.

As part of this enhancement, the following updates are introduced:

- The interface now includes new fields that indicate the time of the last successful sync.
- A new alarm generates whenever a syncing failure occurs. The system attempts a resync automatically.
- A new service parameter enables an automatic restart of the Cisco Intercluster Sync Agent, while also allowing backward compatibility with earlier releases.

User Interface Updates

The **Intercluster Peer Configuration** window now displays a new **Last Synchronized Time** status that displays the last successful intercluster peer sync.

Alarm Updates

A new alarm is introduced: **InterClusterSyncAgentPeerPeriodicSyncFailure**. This alarm generates whenever the Cisco Intercluster Sync Agent service detects a periodic sync failure with an intercluster peer. No action is required as the Cisco Intercluster Sync Agent service attempts to resync immediately on failure.

Service Parameter Updates

A new service parameter for the Cisco Intercluster Sync Agent is introduced: **Enable Auto Recovery for Inter-cluster Peer Periodic Syncing Failure**. When this service parameter is enabled, Cisco Intercluster Sync Agent service automatically restarts when any intercluster peer syncing issue is detected. The service parameter is enabled by default but can be disabled to maintain backward compatibility with earlier releases that do not contain this feature.

Jabber Configuration File Management

Starting with Release 12.5(1), you can centrally manage Jabber client configuration parameters using the Cisco Unified CM Administration interface. This feature allows you to create multiple Jabber Client Configuration templates for various deployment scenarios, for example, per site or per user group in a deployment. This feature simplifies Jabber deployment by eliminating the following:

- The need for manual configuration of the jabber-config.xml file.
- The need for upload of configuration file to the TFTP server.
- Restart of the Cisco TFTP service.

Note This feature requires Cisco Jabber 12.5 release version or higher.

User Interface Updates

To support this feature, the UC Service Settings (use the **User Management** > **User Settings** > **UC Service**) window has been updated to include the following new service:

- Jabber Client Configuration (jabber-config.xml)

Using the new service, you can create multiple Jabber Client Configuration templates as per your deployment needs. Each template allows you to configure single, multi-part, and custom parameters. Once the templates are created, navigate to **User Settings > Service Profiles** to associate them to Common, Desktop, and Mobile Jabber client types.

For more information about the different parameters, see the *Parameters Reference Guide for Cisco Jabber*.

Online CA for Certificate Authority Proxy Function (CAPF)

With this release, the Certificate Authority Proxy Function (CAPF) service includes an Online CA option. With the Online CA option, the CSR process is built into Unified Communications Manager. Consequently, CA-signed LSC certificates can be automatically requested and received from a third-party CA in seconds.

In previous releases, the Offline CA option allowed you to request issue CA-signed LSC certificates, but this was a lengthy and manual process. This feature makes it easy to manage phone LSC certificates that are signed by a third-party CA. The Online CA feature reduces significantly the amount of work involved in obtaining CA-signed LSC certificates.

In Release 12.5(1), only Microsoft CA is supported as an Online CA with CAPF.

Configuration

For details on how to configure the Certificate Authority Proxy Function to use an Online CA, see the Certificate Authority Proxy Function chapter of the *Security Guide for Cisco Unified Communications Manager*.

User Interface Updates

The following Cisco Certificate Authority Proxy Function service parameters are updated:

- Certificate Issuer to Endpoint- To support the Online CA feature, this service parameter now includes an **Online CA** option. This option must be selected to use an Online CA.

In addition, the following new service parameters allow you to configure the connection to the CA:

- Online CA Hostname
- Online CA Port
- Online CA Template
- Online CA Type- Currently **Microsoft CA** is the only available third-party CA
- Online CA Username
- Online CA Password

Serviceability Updates

The **Cisco Certificate Enrollment Service** is added as a feature service under the **Security Settings** heading. This service must be operational to use an Online CA.

Cisco Unified Reporting Updates

A new report, **Stale LSCs**, has been added to the Cisco Unified Reporting user interface. This report lists the Locally Significant Certificates (LSCs) that are rejected by the phone.

Command Line Interface Updates

The following CLI commands have been added to the system. These commands work for all three CAPF modes.

- **utils capf stale-lsc delete all**- It deletes all stale-LSC certificates from the system.
- **utils capf stale-lsc view**- It provides a list of all stale LSC certificates.
- **utils capf csr list**- It obtains a timestamped list of pending CSR files from the system. The **list** parameter is added to the existing utils capf csr command.
- **utils capf set keep_alive**- It allows you to set the keepalive timer to ensure that the connection from the phone to CAPF (port 3804 by default) is not timed-out by a firewall. The default setting is 15 minutes.

For additional information, see the Utils Commands chapter of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions, Release 12.5(1)*.

Troubleshooting Updates

The following logs are available:

- CAPF log files are located at: `"/var/log/active/cm/trace/capf/sdi"`. You must enable trace of CAPF service to obtain these logs.
- Cisco RA log files are located at: `"/var/log/active/cm/trace/capf/sdi/nginx<number>.txt"`. There is no need to enable trace to obtain these logs.
- CLI logs are located at: `"/var/log/active/platform/log/cli*.log"`

Managing Default CA Certificates

With this release, you can manage the default CA certificates that are bundled with Unified Communications Manager and IM and Presence Service with ease by using CLI. You have the option to enable or disable the default CA certificates individually or simultaneously. In addition, you can view the purpose of each of these certificates.

Beginning from 12.5(1) release, if you delete a CAPF-trust certificate from a single node using Cisco Unified OS Administration, the certificate is deleted from all servers in the cluster.

CLI Updates

To support this feature, the following CLI commands are new for this release:

show cert default-ca-list
This command displays all the default CA certificates, which are bundled Cisco Unified Communications Manager and IM and Presence Service.

set cert default-ca-list enable { all | common-name }
This command enables all or particular default CA certificates on all servers in the cluster.

set cert default-ca-list disable { all | common-name }
This command disables all or particular default CA certificates from all servers in the cluster.

For more details about CLI commands, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

For more details about Delete a Trust Certificate, see the "Certificate Overview" chapter of the *Security Guide for Cisco Unified Communications Manager*.

Multi-fork Recording using CUBE Media Proxy Server

Prior to Cisco Unified Communications Manager, Release 12.5(1), the Unified Communications Manager supported only single recorder for a call. With the Cisco Unified Communications Manager, Release 12.5(1), the Unified Communications Manager supports Multi-forking for Call Recording feature.

The Unified Communications Manager is connected to CUBE Media Proxy server which is connected to multiple recorders. The JTAPI interface is enhanced to get the details of multiple recorders in case of Multi-Forking recording through CUBE Media Proxy server.

Backward Compatibility

This feature is backward compatible. JTAPI supports the current APIs.

Multiple Login Behavior for Extension Mobility and Extension Mobility Cross Cluster

With this release, the Extension Mobility Cross Cluster feature has been updated. Now, the Extension Mobility Cross Cluster multiple login behavior is consistent with the Extension Mobility multiple login behavior. You can configure **Multiple Login Behavior** in the **Service Parameter Configuration** page as one of the following:

- Multiple Logins Allowed
- Multiple Logins Not Allowed
- Auto Logout

User Interface Updates

In the **Service Parameter Configuration** window, the **Intra-cluster Multiple Login Behavior** service parameter is renamed to **Multiple Login Behavior**. This parameter is applicable to both Extension Mobility and Extension Mobility Cross Cluster logins.

For more information, see the “Extension Mobility” chapter or the “Extension Mobility Cross Cluster” chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/

en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Multiple Secure SIP Trunks to the Same Destination

This release supports the configuration of multiple secure SIP trunks with the same **Destination IP Address** and **Destination Port Number**.

The feature provides the following benefits:

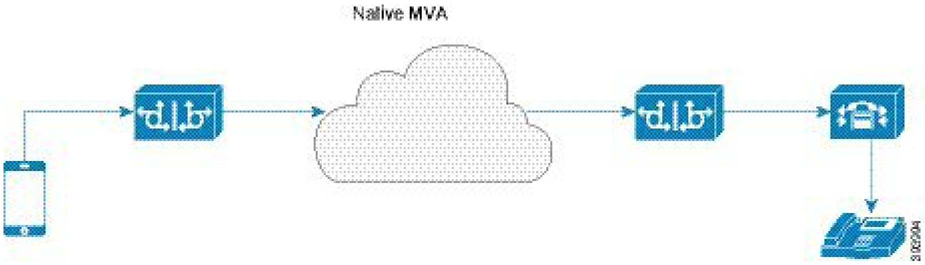
- Bandwidth Optimization: Route for emergency calls with unrestricted bandwidth.
- Selective Routing based on Particular Region or CSS configuration.

Native Mobile Voice Access

This release introduces native support for Mobile Voice Access. This update simplifies your mobility deployment as there is no longer a need to deploy and configure an ISR G2 router to host the Mobile Voice Access IVR—Cisco Unified Communications Manager can host the IVR service natively.

When Mobile Voice Access is configured, end users can call into a system IVR from any phone (for example, a mobile phone or a remote PSTN phone) and after authenticating, place calls that will be routed from that user’s enterprise number. To the called party, the call appears as if the caller were dialing from their own desk phone. In addition, Mobile Voice Access calls are anchored in the enterprise, providing added benefits such as centralized billing, CDR records, and potential cost savings from routing calls over enterprise networks instead of cellular networks.

The following diagram highlights the native Mobile Voice Access setup with a mobile phone. This setup involves two Session Border Controllers, Cisco Unified Communications Manager, and an enterprise desk phone. When the mobile phone user dials in to the IVR number, Cisco Unified Communications Manager authenticates the user, associating the user with the enterprise phone, so that an outgoing call can be placed as if it were dialed from the enterprise desk phone.



Configuration

The principal difference in configuring native Mobile Voice Access support, compared to legacy Mobile Voice Access is as follows:

- There is no longer a need to deploy an ISR G2 gateway to handle voice prompts.

- The Mobile Voice Access Number service parameter represents the directory number that customers must dial to gain access to Mobile Voice Access prompts. This number is for Mobile Voice Access only and cannot be assigned as a directory number to a user phone line.
- After configuring the system for Mobile Voice Access, restart the **Cisco CallManager** service.

For full details on how to set up Mobile Voice Access, refer to the Mobile Voice Access configuration topics of the “Configure Cisco Unified Mobility” chapter in the Feature Configuration Guide for Cisco Unified Communications Manager.

Native and Legacy Mobile Voice Access Integration Option

If you have an ISR G2 router deployed, you still have the option to deploy legacy Mobile Voice Access where requests to the IVR are sent to an ISR G2 router with VXML support. You can integrate both methods of Mobile Voice Access within a single system. This is because the Mobile Voice Access Number service parameter that is configured in Cisco Unified Communications Manager does not have to match the value of the External Number that is defined in the dial peer on the router.

There are a couple options for integrating both native and legacy MVA in your cluster. For example:

- Configure different Mobile Voice Access (MVA) numbers for native and legacy support. Users will use the MVA service that corresponds to which number they dial. If they dial the legacy MVA number that is configured on the router, they will use the legacy MVA service from the ISR G2 router. If they dial the number that is configured in the Mobile Voice Access Number service parameter, they will be routed via Cisco Unified Communications Manager native MVA support.
- Deploy multiple Session Border Controllers with the same number. Users may use either MVA method depending on how the system routes them.

Persistent Chat Support on Jabber Mobile

This release supports persistent chat rooms for Cisco Jabber on iPhone, iPad, and Android. This update allows Cisco Jabber mobile clients to enjoy the exact same persistent chat functionality as desktop clients such as Cisco Jabber on Windows or Mac.

This feature includes no changes to the way persistent chat rooms are configured on the IM and Presence Service. However, the feature includes the following updates for Cisco Jabber on iPhone, iPad, and Android:

- Cisco Jabber mobile clients can now enter persistent chat rooms.
- The Mute function, which can be used to disable persistent chat notifications while Jabber is in silent mode. The Mute feature must be enabled by Cisco Jabber users from within their Cisco Jabber client.
- The Mentions feature, which overrides the Mute setting. If a Jabber user is mentioned, they will receive a notification, regardless of whether they've activated the Mute feature.
- Behind the scenes notifications to your other Jabber applications so that when you read a chat message on one device, it appears as a read message for all of your Jabber applications.

Minimum Release Support

The following minimum release support information applies for this feature:

Product	Support Information
IM and Presence Service	• For the 11.x set of releases, this feature is introduced with 11.5(1)SU5. For the 12.x set of releases, this feature will be introduced with 12.5(1). • If you have this feature deployed in 11.5(1)SU5 and you want to upgrade to a 12.x release, you must upgrade to 12.5(1) to maintain support for this feature. Persistent Chat for Jabber mobile clients is not supported with Release 12.0(1) or 12.0(1)SU1.
Cisco Jabber	• The minimum Cisco Jabber release is 12.1(0). • For additional information on Cisco Jabber functionality, refer to your Cisco Jabber documentation.

Configuration

For details on how to configure Persistent Chat, refer to the "Configure Chat Rooms" chapter of the *Configuration and Administration Guide for the IM and Presence Service*.

Remote Account Security Enhancements

The Remote Account feature is enhanced to use an asymmetric-based encryption model with a public and private key pair for the passphrase. This update enhances the security of your system by ensuring that your system is not accessed by an intruder through the Remote Account. Only Cisco TAC personnel is able to decode the passphrase, allowing access to your system through the Remote Account.

Note This feature is also supported in Unified Communications Manager Release 10.5(2)SU7, 11.5(1), and 11.5(1)SU4.

Setting Up a Remote Account

If you are opening a case with TAC, and you must allow remote access to your system, obtain the Remote Account information from the **Remote Access Configuration** window in the Cisco Unified Operating System Administration interface, or by running the `utils remote_account status` CLI command.

For details on how to set up a remote account, see the "Set up a Remote Account" procedure in the "Opening a Case with TAC" chapter of the *Troubleshooting Guide for Cisco Unified Communications Manager*. Alternatively, you can use the Command Line Interface to set up a remote account. For details, see the `utils remote_account *` commands in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Troubleshooting Logs

The following troubleshooting logs are available for this feature:

- The Remote Support UI logs are located at: `/usr/local/thirdparty/jakarta-tomcat/logs/cmplatform/log4j/cmplatform*.log`

- The Remote Support CLI logs are located at: `"/var/log/active/platform/log/cli*.log"`
- The Remote Support create account logs are located at: `"/var/log/active/platform/log/createaccount*.log"`

RFC 2833 DTMF Support on ISR Gateway-Based SCCP Conference Bridges

As of Release 12.5(1), Unified Communications Manager supports in-band RFC 2833 Dual Tone Multi-Frequency (DTMF) on ISR Gateway-based Skinny Client Control Protocol (SCCP) conference bridges. With this update, SCCP conference bridges can provide seamless support for in-band DTMF and out-of-band DTMF.

This feature removes the need to insert a Media Termination Point (MTP) for DTMF interworking. In previous releases, when only out-of-band DTMF was supported, Unified Communications Manager allocated an MTP in scenarios where a conference participant supported only in-band RFC 2833 DTMF. The MTP allocation required additional media resources and compromised security. This feature update addresses this issue.

RFC 2833 is supported only for Cisco 4000 Series ISR Gateway-based SCCP conference bridges. The Cisco 4000 Series ISR Gateway must be running a minimum release of 16.7.1. For older conference bridges that support only out-of-band DTMF, Unified Communications Manager does not advertise in-band support.

Search Conference Rooms via UDS Proxy for LDAP

As a part of this release, UDS Proxy feature is enhanced to support conference rooms represented as Room objects search in OpenLDAP Server. When no filter is set and the directory server type is OpenLDAP, Unified Communications Manager searches for users only using the default filter string (objectclass=inetOrgPerson). To search conference rooms, configure the custom filter with filter string (|(objectClass=intOrgPerson)(objectClass=rooms)) and use this custom filter in LDAP Search Settings.

This allows Cisco Jabber client to search conference rooms by their name and dial the number associated with the room. Conference rooms are searchable provided givenName, sn (lastName), mail, displayName, or telephonenumber attribute is configured in the OpenLDAP server for a room object.

This feature enhances the existing tokenizing rule for **name** search with search string containing multiple words with spaces. For example, when searching for a string A B C D with three spaces:

1. Searches the entire string (A B C D) as the First name.
2. Searches the entire string (A B C D) as the Last Name.
3. Searches the first word (A) as First Name and the remaining words (B C D) as the Last Name.
4. Searches the first word (A) as Last Name and the remaining words (B C D) as the First Name.

Device Onboarding with Activation Codes

Activation codes make onboarding newly provisioned phones easy. An activation code is a single-use, 16-digit value that a user must enter during phone registration. Activation codes provide a method for provisioning and onboarding phones without requiring an administrator to collect and input the MAC Address for each phone.

Activation codes provide the following benefits:

- No need to manually enter actual MAC addresses. Administrators can use dummy MAC addresses and the phone updates the configuration automatically with the real MAC address during registration.
- No need to deploy an IVR, such as TAPS, to convert phone names from BAT to SEP.

Phone users can obtain their activation codes via the Self-Care Portal, provided the **Show Phones Ready to Activate** enterprise parameter is set to **`True`**. Otherwise, administrators must provide the codes to phone users.

Note When you provision with dummy MAC addresses, activation codes are connected to the phone model. You must enter an activation code that matches the phone model in order to activate the phone.

For added security, you can provision the phone with the phone's actual MAC address. This option involves more configuration because the administrator must gather and input each phone's MAC address during provisioning, but provides greater security because users must enter the activation code that matches the phone's actual MAC address.

Phone Model Support

With Release 12.5(1), activation codes are supported for the following Cisco IP Phone models: 7811, 7821, 7832, 7841, 7861, 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, and 8865NR.

Configuration

For details on how to configure and use this feature, see the "Device Onboarding with Activation Codes" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*.

User Interface Updates

To support this feature, the following updates have been made:

- The **Onboarding Method** field has been added to the **Device Defaults** window. This field must be set to **Activation Code** for activation codes to be used. If this is configured, those phone models will use activation codes instead of autoregistration for onboarding.
- The **Phone Configuration** window has been updated with the following fields:
  - **Requires Activation Code**- When this check box is selected, the phone requires an activation code to onboard.
  - **View Details**- Click this button to view the account details.
  - **Generate New Activation Code**- Click this button if you have an active activation code and want to generate a new one.
  - **Release Activation Code**- Click this button to remove the activation code.
- The **Export Activation Codes** option has been added to the **Related Links** from the **Find and List Phones** window. You can use this option to output the list of active Activation Codes to a CSV file.

- The **Require Activation Code for Onboarding** option has been added to the BAT Template in the Bulk Administration Tool.

Self-Care Portal Updates

The phone display in the Self-Care Portal now includes a **Ready to Activate** option that allows phone users to activate their phones via the Self-Care Portal. This option displays if the phone has not been activated and requires an activation code for activation. When a user clicks this option, they see the activation code that is associated with the phone. They can activate their phone by entering the code on the phone or by using the phone's camera to scan the activation code barcode.

To use this method, the **Show Phones Ready to Activate** enterprise parameter must be set to **True** in Unified Communications Manager.

Serviceability Updates

To support this feature, the **Cisco Device Activation Service** has been added. This feature service is enabled by default.

Alarm and Counter Updates

The new alarm, **DevActApplicationOnboardIssue**, is added for this release. This alarm is triggered whenever device activation fails. This alarm has two possible causes: model mismatch or hostname mismatch. It's recommended to generate a new activation code before retrying device onboarding.

The following new counters were added under the Cisco Device Activation Service:

- **ActivationCodeAttempts**- This represents the number of activation code creation requests.
- **ActivationCodeFails**- This represents the number of failed activation code creation requests. Failure reasons include DB errors such as one code per phone record only. API is rate limited.
- **InvokeAttempts**- This represents the number of invoke requests. Phone started SRP handshake to onboard.
- **InvokeFails**- This represents the number of failed invoke requests. Failure reasons include server is busy, API is rate limited, or bad activation code received.
- **RegisterAttempts**- This represents the number of register requests. Phone is finishing SRP handshake to onboard.
- **RegisterFails**- This represents the number of failed register requests. Failure reasons include server is busy, API is rate limited, model mismatch, device name mismatch, or bad MIC.
- **ReleaseAttempts**- This represents the number of activation code release requests. Release of an activation code is attempted.
- **ReleaseFails**- This represents the number of failed activation code release requests. Failures include API is rate limited and activation code does not exist.
- **ThrottleCount**- Counts the number of times any API failed due to rate limiting. This goes back to zero every minute to see when throttling occurred.

Secure End Users Login Credentials

In previous releases, local end users' login credentials on Unified Communications Manager are hashed using SHA1. From 12.5(1) release onwards, all local end users' login credentials are hashed using SHA2 to provide more security. All local end users' passwords or PINs are migrated to use the new SHA2 standard automatically after their first successful login.

With this release, Unified Communications Manager includes the "**UCM Users with Out-Of-Date Credential Algorithm**" report. This report, which can be accessed from the Cisco Unified Reporting page, helps the administrator to list all the end users' whose passwords or PINs are hashed using SHA1.

User Interface Updates

A new report titled, "**UCM Users with Out-Of-Date Credential Algorithm**" has been added to the **System Report** menu of the Cisco Unified Reporting interface.

Online Help Updates

The following table displays the online help updates for the Secure End Users Login Credentials feature. The reports are the same for Unified Communications Manager and IM and Presence Service.

Table 4: End Users Out-Of-Date Credentials Report

Report	Description
UCM Users with Out-Of-Date Credential Algorithm	Provides a list of local end users' whose passwords or PINs are stored and hashed using SHA1.

For more information about Secure End Users Login Credentials, see the *Security Guide for Cisco Unified Communications Manager*.

External Presentation Name and Number

With release 12.5(1), Cisco Unified CM Administration can be configured to include a separate calling party number and a presentation number. This feature helps users anonymize outbound PSTN calls to show an external presentation name and number instead of their Direct Inward Dial (DID) number that helps reduce robocalls.

The external number cannot be used for billing. Ability to anonymize name and number can be done for an individual user or for a group of users. In previous releases, Unified Communications Manager could not be configured on a per line basis to send a number different than the Direct Inward Dial (DID) number. This feature applies only to PSTN calls. With this release, Unified Communications Manager supports External Presentation Name and Number that is different from existing Identification Name and Number. The configured Presentation Name and Number are for display on the following devices:

- SIP
- SCCP
- SNRD

User Interface Updates

The following user interface updates have been implemented to support External Presentation Name and Number:

- In the SIP Profile Configuration page, **Allow Passthrough of Configured Line Device Caller Information** field is renamed to **Enable External Presentation Name and Number**.
- A new service parameter **Display External Presentation Name and Number** is added under Clusterwide Parameters (Device - Phone) section of **Service Parameter Configuration** page.
- A new section **External Presentation Information** is added with the following three fields on the **Directory Number Configuration** page:
  - Anonymous External Presentation
  - External Presentation Number
  - External Presentation Name
- The following table depicts the existing and renamed fields on the **SIP Profile Configuration** page:

  Table 5: SIP Profile Configuration UI Updates

Existing fields	Renamed fields
Incoming Requests FROM URI Settings	External Presentation Information
Caller ID DN	External Presentation Number
Caller Name	External Presentation Name

  With preceding changes, a new check box **Anonymous External Presentation** is added.
- The following table depicts the existing and renamed fields on the **Trunk Configuration** page:

  Table 6: Trunk Configuration Page UI Updates

Existing fields	Renamed fields
Caller Information	Presentation Information
Caller ID DN	Presentation Number
Caller Name	Presentation Name
Maintain Original Caller ID DN and Caller Name in Identity Headers	Send Presentation Name and Number only in the FROM header and not in the other identity headers check box.

  There is a new check box **Anonymous Presentation**, provided for Administrator to configure anonymous presentation identity.

Session Management

You can limit the maximum number of concurrent web application sessions of a user by using the **set webapp session maxlimit** command. Also, you can terminate a user's active sign-in session specific to each node by entering the user details in the **Session Management** window.

Current Sessions Limit

With this release, Unified Communications Manager limits the maximum number of concurrent web application sessions of a user.

This applies to the following interfaces:

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- Cisco Unified Communications Self-Care Portal
- Cisco Unified Communications Manager IM and Presence Administration
- Cisco Unified IM and Presence Serviceability
- Cisco Unified IM and Presence Reporting

CLI Updates

A new command named **set webapp session maxlimit** is introduced to support session limitation. You must have command privilege level 4 access to run this command.

For more information on the **set webapp session maxlimit** command, see the “Set Commands” chapter in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions, Release 12.5(1)* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Session Termination

With this release, Unified Communications Manager can terminate a user's active sign-in session specific to each node.

This applies to the following interfaces:

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- Cisco Unified Communications Self-Care Portal
- Cisco Unified Communications Manager IM and Presence Administration
- Cisco Unified IM and Presence Serviceability

- Cisco Unified IM and Presence Reporting

User Interface Updates

The **Session Management** window is added to the **Security** menu of the Cisco Unified OS Administration and Cisco Unified IM and Presence OS Administration interfaces.

Session Management Settings

The following table details the **Session Management** window fields:

Field	Description
Status	Displays the session termination status message for the selected user ID.
Terminate Session	
User ID	Enter the user ID of the active signed-in user. This is a required field.
Terminate Session	**Terminate Session** button, terminates the session of the active signed-in user.

For more details on how to configure session termination, see "Manage Security" chapter in the *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 12.5(1)* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Simplified Upgrades

This feature improves the native upgrade experience of Unified Communications Manager and Instant Messaging & Presence Service.

It simplifies the upgrade process by reducing:

- Upgrade duration
- Service impact
- Sequencing complexity
- Manual touch points

Database replication is moved to pre-reboot stage, simplifying change management and reducing user/device impact of post-reboot updates.

You can perform cluster-wide upgrade. One-touch cluster-wide upgrade and reboot controlled by Unified Communications Manager Publisher reduces the manual touch points by 90%, simplifying maintenance window planning and further shortens the overall duration (50% for large systems).

Automated pre-upgrade and post-upgrade COP files allow early detection of issues that could cause upgrade failures.

Prime Collaboration Deployment batch COP install and task chaining reduces manual touch points for multistage operations.

Command Line Interface and User Interface Updates:

The following new options are added in the Unified Communications Manager, and IM and Presence User Interface and the **utils system upgrade initiate** command at the Command Line Interface:

- **Install/Upgrade Cluster** menu is added under **Software Upgrades**. With this option, you can perform cluster-wide upgrade only after completing the download of the upgrade files in all the selected nodes in the cluster.
- **utils system upgrade cluster**- With this new CLI command, you can perform the cluster-wide upgrade through CLI.
- **Reboot Cluster** menu is added under **Software Upgrades**. With this option, you can perform the cluster-wide restart or switch version operation. You can perform the switch version or restart by placing cluster nodes in batches sequentially using the sliders.
- **Local Filesystem** option is added in the **Source** drop-down list under **Install/Upgrade Cluster** and **Install/Upgrade** page.

  Local Image option is displayed in the **utils system upgrade initiate** command in CLI.

  With this Local Image or Local Filesystem source option, you can use a previously downloaded ISO or COP file during the upgrade. If there is no downloaded ISO or COP file, the source displays the Local Image<none>. If there is an ISO or COP file, then it displays the Local Image option with the .iso or.cop downloaded file.
- **Use download credentials from Publisher** option is added in the **Software Installation/upgrade** page of Unified Communications Manager, and IM and Presence User Interface, and in the **utils system upgrade initiate** CLI command. With this option, you can use the source configurations in the publisher. This option is available in Unified Communications Manager subscriber, IM and Presence publisher, or subscriber nodes in a cluster. This option is not applicable for cluster-wide upgrade.
- **Continue with upgrade after download** option is added in **Software Installation/upgrade** page of Unified Communications Manager, and IM and Presence User Interface and in the **utils system upgrade initiate** CLI command. With this option, the upgrade starts automatically after the file downloads. It does not wait for the user confirmation and starts the installation.
- **Switch-version server after upgrade** option is added in **Software Installation/upgrade** page of Unified Communications Manager, and IM and Presence User Interface and in the **utils system upgrade initiate** CLI command. With this option, system reboots automatically after the completion of successful upgrade.

For more information on CLI, see the "utils system upgrade" section of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

For more information, see the "Upgrade the Applications" section of the *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

Serviceability Updates

Platform Communication Web Service is added as a platform service. This service is a Representational State Transfer Protocol (REST) API that runs on Unified Communications Manager, IM and Presence, and Cisco Unity Connection systems.

For more information, see the "Platform Services" of the *Cisco Unified Serviceability Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Pre and Post Upgrade COP Files

In this release, two COP files (pre-upgrade and post-upgrade) are provided that you can use to check the system health and its readiness for upgrade. Any failure in the pre-upgrade COP should be fixed before performing an upgrade.

The COP files run a series of tests and identify issues that can cause upgrade failures and also collects status and value data used to compare the information before and after upgrade. Using the information, you can take corrective action, if required.

For more information, see the "Pre-Upgrade Task Flow" and "Post-upgrade Task Flow" sections of the *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

SIP OAuth Support on Unified Communications Manager

Secure registrations to Unified Communications Manager involves a process of updating CTL files, setting up a mutual certificate trust store and so on. If a Jabber device is switching between on-premises and off-premises, it is cumbersome to update LSCs and renew CAPF enrollment each time a secure registration is made.

Supporting OAuth on the Unified Communications Manager SIP line allows secure signalling and media without CAPF. When OAuth based authorization is enabled on Unified Communication Manager cluster and Jabber endpoint, OAuth token validation during SIP registration is done.

Smart Software Licensing

On 11.5.1, Prime License Manager provides the voucher for onboarding APNS cluster. From 12.x onwards, Cisco Smart Software Manager or Cisco Smart Software Manager Satellite provides the voucher for onboarding APNS cluster, before that APNS cluster should be registered to Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

For more details, see the *Licensing Prerequisites* chapter of https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/push_notifications/cucm_b_push-notifications-deployment-guide/cucm_b_push-notifications-deployment-guide_chapter_01.html#reference_CE836F3E3283BCF699F2AFC21426B783

Specific License Reservation

This is a feature for a highly secure environment with no ability at any time to connect to Cisco Smart Software Manager or Cisco Smart Software Manager Satellite.

Specific License Reservation allows entitlements, perpetual or term, to be reserved for a Unified Communications Manager product Instance. A generated authorization code from Cisco Smart Software Manager can be installed on the Unified Communications Manager product and no regular synchronization is needed if product runs within specified license consumption.

Ability to reserve license on Cisco Smart Software Manager is through Smart Account profile. To enable Specific License Reservation on Smart Account, send email to sa-adoption-support@external.cisco.com.

For details on how to configure Cisco Specific License Reservation, see the “Specific License Reservation” chapter of the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

CLI Updates

The following new CLI commands have been introduced to support this feature:

- license smart reservation enable
- license smart reservation disable
- license smart reservation request
- license smart reservation cancel
- license smart reservation install "<authorization-code>"
- license smart reservation install-file <url>
- license smart reservation return
- license smart reservation return-authorization "<authorization-code>"

For more details about these CLI commands, see the “ License Commands” and “ Show Commands” chapter of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Alarm and Alert Updates

Alert

The following new alerts have been introduced to support this feature:

- SmartLicense_SLR_InEval
- SmartLicense_SLR_NoProvision_EvalExpired
- SmartLicense_SLR_InOverage_NotAuthorized
- SmartLicense_SLR_NoProvision_NotAuthorized

- SmartLicense_SLR_ExportControlNotAllowed

For more details about these alerts, see the " Performance Counters and Alerts" chapter of the *Cisco Unified Real-Time Monitoring Tool Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Export Controlled functionality in Specific License Reservation

To enable the mixed mode or to update the CTLFile, ensure that the Specific License Reservation registration is completed in Unified Communication Manager by using the authorization code received from the Smart account of Cisco Smart Software Manager (CSSM) that has Allow export-controlled functionality configured.

Transport Settings Enhancement

With this release, Smart Account allows the Administrator to checkbox and to restrict IP Address and Hostname of the Unified Communications Manager being exchanged during the registration to Cisco Smart Software Manager or Cisco Smart Software Manager Satellite.

Updating VMware Tools

With this release, Unified Communications Manager supports VMware Tools update on one of the following:

- Native VMware Tools (provided by VMware)
- Open VMware Tools (provided by Cisco)

- To upgrade Unified Communications Manager from a version earlier than Release 12.5(1), you must use the native VMware tools option. You can change to open VMware Tools after the upgrade.
- For upgrades from Unified Communications Manager Release 12.5(1) onwards (for example, to a higher SU), you can choose whether your system use Native VMware or Open VMware Tools.
- For fresh installation and PCD migrations from Unified Communications Manager Release 12.5(1) onwards, open VMware tools installed by default.

For details on how to update VMware tools, see the *"Updating VMware Tools"* chapter of the *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service*

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.