New and Changed Features

The following new and changed feature was introduced for Release 11.5(1)SU7:

- AES 80-Bit Authentication Support, on page 1
- Call Recording for SIP TLS Authenticated calls, on page 1
- Encrypted IM Compliance Database, on page 2
- Immediate Divert to Voicemail for WebEx Hybrid Services, on page 5
- Persistent Chat Support on Jabber Mobile, on page 5
- Push Notifications Updates, on page 6
- Search Conference Rooms via UDS Proxy for LDAP, on page 6

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*.

Call Recording for SIP TLS Authenticated calls

Prior to 11.5(1)SU5 version, the phones that 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 this release 11.5(1)SU5, Cisco Unified Communications Manager allows call recording for authenticated phones while using non secure recorder. In case of secure recorder, recording is allowed only if the recorder supports Secure Real-Time Transport protocol (SRTP) fallback.

To record a call for authenticated phones, On the Cisco Unified Communications Manager Service Parameter page, set the **Authenticated Phone Recording field** to **Allow Recording**. The default value is **Do Not Allow Recording**.

Cisco Unified Communications Manager JTAPI/TAPI interface has been enhanced to allow recording in Authenticated phone, based on the value of the new service parameter - **Authenticated Phone Recording**. Now, the expectation is that the call recording can be done by Authenticated phones also. The value of newly added service parameter can be set as as follows:

- **Allow Recording** – Authenticated phones can record the calls..
- **Do Not Allow Recording** – Authenticated phones cannot record the calls. This will be the default value for the service parameter. The behavior would be the same as that of the current behavior.

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

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 1: 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 2: 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.

Immediate Divert to Voicemail for WebEx Hybrid Services

The SIP trunk messaging specifications are updated to provide support for Immediate Divert to Voicemail from Cisco Webex Hybrid Services. To support this feature on Cisco Webex Hybrid Services, the SIP 603 DECLINE response has been added to the SIP trunk messaging specifications for Cisco Unified Communications Manager.

This update applies only for incoming calls to a Cisco Spark Remote Device. Previously, when a user declined an incoming call to this device type, the call was redirected to the user's enterprise phone. With the 603 Decline response, declined calls can go directly to the user's voicemail.

For information on how to configure this feature for Cisco Webex Hybrid Services, refer to your Hybrid Services documentation.

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*.

Push Notifications Updates

With this release, the behavior of the **Send Troubleshooting Information to Cisco Cloud** check box in the **Cisco Cloud Onboarding** window for the Push Notifications feature has changed as follows:

- Usage Metrics—With this release, Push Notifications usage metrics are now sent to the Cisco cloud once every 24 hours irrespective of the setting of this field. In previous releases, Push Notifications usage metrics were sent to the Cisco cloud only if this check box was checked. Usage metrics consists of the number of successful and failed Push Notifications–no user-generated content, or personally identifiable information, is passed along with these metrics.
- Default Setting—The default setting for this check box is checked. Previously, the default setting was unchecked.
- Alarms—There is no change to the behavior for Push Notifications alarms. Push Notifications alarms will be sent to the Cisco cloud only if this check box is checked.

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.