



New and Changed Features

- [Emergency Call Routing Regulations, on page 1](#)
- [Enhancement to Caller-ID in Call Pickup Notification Toast for Jabber in Deskphone Control Mode, on page 2](#)
- [Extension Mobility Login Simplification using Headset, on page 2](#)
- [Connected Number Display for Forwarded Calls for Jabber in Deskphone Control Mode, on page 2](#)
- [Granular Access Control Enhancements, on page 3](#)
- [Native Phone Migration using IVR and Phone Services, on page 3](#)
- [BFCP Presentation Sharing in Audio Only Call with TRP, on page 4](#)
- [Push Notifications for iOS and Android Clients, on page 5](#)
- [IM and Presence Configuration for SIP Open Federation, on page 6](#)
- [IM and Presence Intercluster Peer Synch Interval, on page 6](#)

Emergency Call Routing Regulations

The US Federal Communications Commission (FCC) has signed the Call Routing Regulations requesting Multi-Line Telephone Systems (MLTS) Systems to provision or enforce direct 911 dial (without any prefix dialing). The Unified Communications Manager is responsible for routing all emergency calls in agreement with the FCC rules.

Unified CM installed or upgraded fully or partly in regions where the FCC rules are applicable, detects the presence of a direct dial 911 Route Pattern and disables further notifications to the administrator.

If the 911 pattern doesn't exist, Unified CM sends an alert notification to an administrator to create the 911 Route pattern.

An administrator must consult their legal counselor on the applicability of the law and acknowledge along with performing necessary configurations or disable further notifications if not applicable. For more information on acknowledging and acceptance of law, see the chapter "The US Federal Communications Commission (FCC) Emergency Call Routing Regulations" in the [Feature Configuration Guide for Cisco Unified Communications Manager](#).

Enhancement to Caller-ID in Call Pickup Notification Toast for Jabber in Deskphone Control Mode

The Caller ID is not shown in the Call Pickup notification toast when Cisco Jabber is in Deskphone control mode and Call Pickup page is configured to not show the caller ID. This makes the experience comparable to Jabber in softphone mode.

Extension Mobility Login Simplification using Headset

The Extension Mobility using headset feature that was introduced in Release 11.5(1)SU8 is carried over to 12.5(1)SU3 release. The following are additional updates introduced in this release:

- Administrator can associate headset to users from the Headset Inventory page.
- There is an administrator-controlled option to log in to Extension Mobility service using the headset without requiring a user PIN. This enables touchless login to the Extension Mobility service.

For more information, see 'Enable Pinless Extension Mobility Login' and 'Associate Phone Owner as Headset Owner' sections of the 'Headset Service' chapter in [Feature Configuration Guide for Cisco Unified Communications Manager](#).

User Interface Updates

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

1. In the **System > Enterprise Parameters Configuration** page, a new parameter **PIN entry for headset-based sign in** is added to enable or disable pinless Extension Mobility login.

The following options are available in the new parameter:

- Required
- Not Required

2. In the **Device > Headset > Headset Inventory** page, two new options are added to associate or disassociate bulk headsets to the user.

The following are the options:

- Associate Phone Owner as Headset Owner
- Disassociate Headset Owner

Connected Number Display for Forwarded Calls for Jabber in Deskphone Control Mode

In this release, Cisco Jabber in Deskphone control mode honors the "Always Display Original Dialed Number" Service Parameter configured in the Cisco Unified Communication Manager Administration user interface.

When this parameter is configured, original dialed number is displayed as connected number on caller's display. This ensures that user's privacy settings are honored.

Granular Access Control Enhancements

Granular Access Control Enhancements allows creation of hierarchy among administrators for segregation of duties. This enhancement allows the higher ranked user to view or modify the permission information or user rank of same or lower ranked users but not vice versa.

User Interface Updates

The following fields are introduced:

- In the **User Management > User Settings > Roles** page, two new fields are added under the **Advanced Role Configuration** window.
 - **User can update Permissions Information for own user**
 - **User can update User Rank for own user**

For more information, see the *Cisco Unified CM Administration Online Help*.

Native Phone Migration using IVR and Phone Services

The Phone Migration feature is an easy and intuitive Cisco IP Phone migration solution native to Unified Communications Manager. It minimizes the cost and complexity of replacing deprecated or faulty phones. Using this solution, an end user or an administrator can easily migrate all the settings from an old phone to a new phone with a simple user interface. Solution supports the following methods for migration of the phones:

- **Using Self-provisioning IVR Service**
- **Using Phone Migration Service**
- **Using Cisco Unified CM Administration Interface**

Following table provides a quick comparison of the various phone migration options:

Table 1: Different Phone Migration Options and Considerations

	Using Self-provisioning IVR Service	Using Phone Migration Service	Using Unified CM Administration Interface
End user or administrator driven phone migration	End user (Self-service)	End user (Self-service)	Administrator
Auto-registration required	Yes	No	No

	Using Self-provisioning IVR Service	Using Phone Migration Service	Using Unified CM Administration Interface
Migration steps	<ul style="list-style-type: none"> • Auto register a new phone • Dial self-provisioning IVR number • Follow the voice prompts 	<ul style="list-style-type: none"> • Plug-in new phone to the network • Key in primary extension and PIN (optional) 	<ul style="list-style-type: none"> • Sign in to Cisco Unified CM Administration interface • Choose “Migrate Phone” option in the Phone Configuration page of the old phone • Enter phone type (model & protocol) and MAC address of the new phone
Administrator involvement	Medium	Low	High

For more information, see the “Native Phone Migration using IVR and Phone Services” chapter in the [Feature Configuration Guide for Cisco Unified Communications Manager](#).

User Interface Updates

The following fields are added:

- In the **System > Enterprise Parameters Configuration** page, a new section **Phone Migration** is added. The following options are available in the new section:
 - **When Provisioning a Replacement Phone for an End User** drop-down list is added.
 - **Security Profile for Migrated Phone** drop-down list is added.
 - **Phone Migration User Identification Prompt** drop-down list is added.
- In the **User Management > User Settings > User Profile Configuration** page, a new check box is added under the **Self-Provisioning** section.
 - **Allow Provisioning of a phone already assigned to a different End User**
- In the **Find and List Phones Configuration** page, a new drop-down list **Migrated (old phone)** is added.

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

BFCP Presentation Sharing in Audio Only Call with TRP

Unified Communication Manager supports BFCP-based presentation sharing when two video capable devices start a call in Audio Only mode and there is a TRP in the media path.

For more information, see the “Configure Presentation Sharing using BFCP” chapter in the [Feature Configuration Guide for Cisco Unified Communications Manager](#).

Push Notifications for iOS and Android Clients

This release includes a number of updates and changes for Push Notifications deployments.

Apple Push Notifications Updates

As of August 2020, legacy VoIP mode is now disabled for Cisco Jabber on iPhone and iPad clients, making Push Notifications a mandatory deployment for Cisco Jabber on iPhone and iPad clients.

Apple Push Notifications support for Cisco Jabber and Cisco Webex clients that run on iOS devices is updated to meet new Apple requirements and also to support iOS 13 SDK updates. Updates include:

- Caller ID in the Push Notifications—Cisco Jabber and Cisco Webex clients now launch CallKit with Caller ID once the Push Notification is received, rather than when the SIP INVITE is received. The Caller ID supports External Presentation Name and Number, if it is configured on Unified Communications Manager.
- Active Registration node—Push Notifications now include the IP address of the node which generates the Push Notification. This update prevents delay in registration if the node to which the client was registered previously restarts while the client is in the background. With this change, the client can quickly register to the node that generates Push Notification and is in a healthy state.
- Push Notifications support in China—This release supports changes that are required for Apple devices in the China region so that the Cisco Jabber or the Cisco Webex client complies with local government regulations about VOIP applications not showing CallKit. Note that Cisco Jabber version 12.9MR is required for users in China Region.



Note These updates assume that you have updated Cisco Jabber to 12.9. If you are running earlier Jabber versions, Push Notification will not include the Apple Push Notification service changes that are included in iOS 13.

For more information on iOS 13 requirements for Push Notifications, see the section [Apple Push Notifications Service Updates](#).

Android Push Notifications Support Introduced

This release introduces Push Notifications support for Cisco Jabber and Cisco Webex clients that run on Android devices. Android Push Notifications feature support includes:

- Active Registration node—Push Notifications include the IP address of the node which generates the Push Notification. This update prevents a delay in registration if the node to which the client was registered previously restarts while the client is in background mode. With this change, the client can quickly register to the node that generates the Push Notification and is in a healthy state.



Note For Cisco Webex clients, only voice push notifications are supported.



Note Android Push Notifications do not support Caller ID within the Push Notification. The CallKit launches only when the client receives the SIP INVITE. In addition, Android Push Notifications are not supported in China.

Push Notifications Deployment and Configuration

For detailed information on how to deploy and configure Push Notifications for either Android or iOS clients, see the [Push Notifications Deployment Guide](#).

IM and Presence Configuration for SIP Open Federation

Cisco IM and Presence Service supports SIP open federation for Cisco Jabber clients. As an administrator, you can configure SIP open federation allowing Cisco Jabber users to seamlessly federate with users from domains that support SIP based federation. This feature establishes the co-existence of open IM federation for both SIP and XMPP clients in the IM and Presence server. Unlike in Controlled SIP Federation where you must configure each federated domain separately, you can configure open federation for all domains with a single pre-configured static route. The static route lets Cisco Jabber federate with any external domain. More importantly, it significantly cuts down the time to configure and maintain SIP federation for individual domains.

For configuration information, see the "IM and Presence Configuration for SIP Open Federation" chapter in the [Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager Guide](#).

IM and Presence Intercluster Peer Synch Interval

IM and Presence Service allows you to set time interval for intercluster peer syncing. The newly introduced service parameter **Inter Cluster Peer Periodic Sync Interval (mins)** allows you to configure the time interval for dynamic ICSA periodic sync from **Cisco Unified CM IM and Presence Administration** user interface. If the intercluster peer sync fails, then ICSA service restarts.

For detailed information on how to configure intercluster peer sync interval, see chapter 'Configure Intercluster Peers' in [Configuration and Administration of the IM and Presence Service](#).