Release Notes for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5(1)SU2

First Published: 2016-10-21

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **About this Release** 1

About Release Notes 1

Supported Versions for 11.5(1)SU2 2

Supported Platforms 2

Documentation for Release 11.5(1)SU2 2

CHAPTER 2 **Upgrades** 5

Upgrading your System 5

Version Requirements 5

Supported Upgrade and Migration Paths 6

Applications Installed on Cisco Media Convergence Servers Hardware 6

Applications Installed on Virtual Machines 7

COP Files Required for Upgrades to Release 11.5 8

Rolling Back to Previous Versions 10

Upgrading with FIPS Mode Enabled 10

Deprecated Phone Models 10

OS Admin Account Required for CLI-Initiated IM and Presence Upgrades 11

CHAPTER 3 **New and Changed Features** 13

Cisco Meeting Server Conference Bridge 13

Cisco Spark Remote Device 14

Configure a Cisco Spark Remote Device 14

Configure a Cisco Spark Remote Device 14

Cisco Spark Remote Device Configuration Fields 15

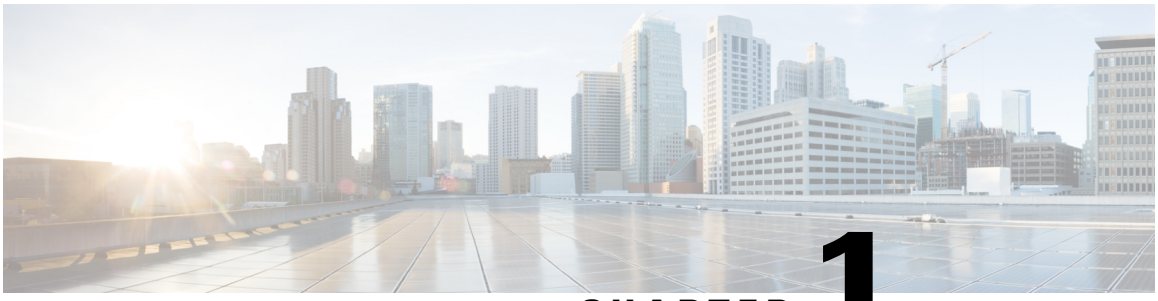
Add a Directory Number to a Cisco Spark Device 19

Cisco Spark Remote Device Licensing 19

Federation with Skype for Business 20

IM and Presence Service Ad hoc Chat Room Discovery 20

Log Compression for IM and Presence Service 20
Push Notifications with Cisco Jabber for iPhone and iPad 21
Performance Counters for Push Notifications 22
Rosters Cleanup for IM and Presence 26
Delete Invalid Contacts and Watchers 27
Persistent Chat High Availability 27
MRA Support for Shared Line 28
Feature Limitations For MRA Endpoints 28
TLS as a Communication Protocol for Common Criteria Compliance 29



CHAPTER 1

About this Release

- About Release Notes, page 1
- Supported Versions for 11.5(1)SU2, page 2
- Supported Platforms, page 2
- Documentation for Release 11.5(1)SU2, page 2

About Release Notes

These release notes describe new features, requirements, restrictions, and caveats for Cisco Unified Communications Manager and IM and Presence Service. These release notes are updated for every maintenance release but not for patches or hot fixes.

Unified Communications Manager, the call-processing component of the Cisco Unified Communications System, extends enterprise telephony features and capabilities to IP phones, media processing devices, VoIP gateways, mobile devices, and multimedia applications.

IM and Presence Service collects information about user availability, such as whether users are using communications devices (for example, a phone) at a particular time. IM and Presence Service can also collect information about individual user communication capabilities, such as whether web collaboration or video conferencing is enabled. Applications such as Cisco Jabber and Unified Communications Manager use this information to improve productivity among employees, that is, to help employees connect with colleagues more efficiently and determine the most effective way to engage in collaborative communication.

Note In the past, export licenses, government regulations, and import restrictions have limited the ability of Cisco to supply Unified Communications Manager and IM and Presence Service worldwide. Cisco has obtained an unrestricted U.S. export classification to address this issue; IM and Presence Service supports an export unrestricted (XU) version only. The unrestricted version differs from previous releases of IM and Presence Service in that it does not contain strong encryption capabilities.

Be aware that after you install an unrestricted release, you can never upgrade to a restricted version. You are not allowed to perform a fresh installation of a restricted version on a system that contains an unrestricted version.

Supported Versions for 11.5(1)SU2

The following software versions are supported with Release 11.5(1)SU2:

- Cisco Unified Communications Manager 11.5.1.12900-21
- IM and Presence Service 11.5.1.12900-25

Version Mismatch Not Supported

For your 11.5(1)SU2 deployment to be supported, both Cisco Unified Communications Manager and IM and Presence Service must be running 11.5(1)SU2 versions. Running an 11.5(1)SU2 version of Cisco Unified Communications Manager with an earlier version of IM and Presence Service is not supported. Similarly, running an 11.5(1)SU2 version of IM and Presence Service with an earlier version of Cisco Unified Communications Manager is not supported.

Supported Platforms

This release of Cisco Unified Communications Manager has been tested with, and supports the following operating systems:

- Microsoft Windows
- Linux

Documentation for Release 11.5(1)SU2

Release 11.5(1)SU2 reuses documentation from the 11.5(1) and 11.5(1)SU1 releases. Where an 11.5(1)SU2 document version exists, use the SU2 document. If there is no SU2 version, but there is an SU1 version of a document, use the SU1 version. Otherwise, use the existing document from the 11.5(1) release.

11.5(1)SU2 Documents

Refer to the following Readme files for caveats, bug fixes and important notes that are associated with the 11.5(1) SU2 release:

- Readme File for Cisco Unified Communications Manager, Release 11.5(1)SU2
- Readme File for Cisco Unified IM and Presence Service, Release 11.5(1)SU2

In addition to Release Notes, the following documents were published with new versions for 11.5(1)SU2:

- Interdomain Federation Guide for IM and Presence Service, Release 11.5(1)SU2
- Partitioned Intradomain Federation Guide for IM and Presence Service, Release 11.5(1)SU2

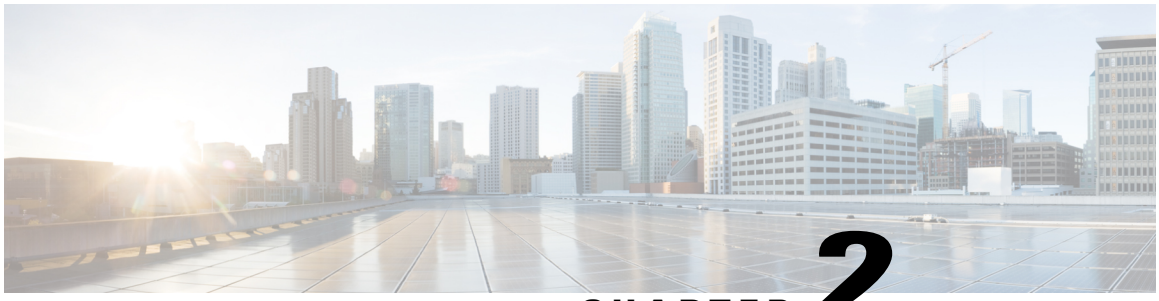
The 11.5(1)SU2 release introduces the Push Notifications feature with Cisco Jabber for iPhone and iPad. The following solution document describes how to set up Push Notifications for an on-premise IM and Presence Service deployment:

- Deploying Push Notifications for iPhone and iPad with the IM and Presence Service and WebEx Messenger

Existing Documentation from Release 11.5(1)

For information on the documentation set that is available for Release 11.5(1) of Cisco Unified Communications Manager and IM and Presence Service, refer to the following document. These documents can be reused for the 11.5(1)SU2, except where an 11.5(1)SU2 version of the document exists:

- Documentation Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5(1)



CHAPTER 2

Upgrades

- Upgrading your System, page 5
- Version Requirements, page 5
- Supported Upgrade and Migration Paths, page 6
- Rolling Back to Previous Versions, page 10
- Upgrading with FIPS Mode Enabled, page 10
- Deprecated Phone Models, page 10
- OS Admin Account Required for CLI-Initiated IM and Presence Upgrades, page 11

Upgrading your System

Refer to the topics in this chapter for supported upgrade paths, migration paths and required COP files to upgrade to Release 11.5(1)SU2. For detailed instructions on how to upgrade your system, refer to the *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 11.5(1)* at the following URL:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/upgrade/11_5_1/cucm_b_upgrade-guide-cucm-115.html

Version Requirements

All servers in a cluster must run the same release of Cisco Unified Communications Manager. The only exception is during a cluster software upgrade, during which a temporary mismatch is allowed.

If you are installing IM and Presence nodes, the software version of the first IM and Presence node (the IM and Presence database publisher node) must match the first two numbers of the software version installed on the Unified Communications Manager publisher node. For example, IM and Presence Service software version 11.0.1.10000-1 is compatible with Cisco Unified Communications Manager software version 11.0.1.30000-2.

After you install the first IM and Presence node, the software version of any IM and Presence subscriber nodes that you install must match all five version numbers of the first IM and Presence node.

For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must also be 11.5.1.10000-1.

Supported Upgrade and Migration Paths

Use the tables below to determine whether you can upgrade or migrate from your currently installed version, and which of the supported upgrade methods are available to you:

- direct upgrades using either the Cisco Unified CM OS Admin interface or the Cisco Prime Collaboration Deployment (PCD) Upgrade task
- migrations using the PCD Migration task

If an upgrade or migration from your current release is not supported, see the instructions in the "Upgrading from Legacy Releases" chapter of the *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service*.

Applications Installed on Cisco Media Convergence Servers Hardware

Applications Installed on Cisco Media Convergence Server (MCS) 7800 Series Hardware

You cannot install or run Cisco Unified Communications Manager and the IM and Presence Service directly on server hardware; you must run these applications on virtual machines. The tables below list the supported migration paths for deployments that are currently running on MCS 7800 hardware. All of the supported migration paths listed below are physical-to-virtual (P2V) migrations.

Note The tables below list the upgrade paths supported for MCS 7800 Series servers, with the following exceptions:

- MCS 7816-C1 for Business Edition 3000 (BE3000)
- MCS 7828 for Business Edition 5000 (BE5000)

PCD migrations are not supported for BE3000 and BE5000 deployments. We recommend a fresh installation for upgrades from these products.

Table 1: Cisco Unified Communications Manager Releases Installed on MCS 7800 Series Hardware

From	To	Supported Method
6.1(5)	11.5(x)	PCD Migration
7.1(3) and 7.1(5)	11.5(x)	PCD Migration
8.x	11.5(x)	PCD Migration
9.x	11.5(x)	PCD Migration

Table 2: Cisco Unified Presence and IM and Presence Releases Installed on MCS 7800 Series Hardware

From	To	Supported Method
CUP 8.5(4)	11.5(x)	PCD Migration
CUP 8.6(3), 8.6(4), and 8.6(5)	11.5(x)	PCD Migration
IM and Presence 9.x	11.5(x)	PCD Migration

Applications Installed on Virtual Machines

Applications Installed on Virtual Machines

The tables below list the supported upgrade and migration paths for deployments that are currently running on virtual machines. All of the supported upgrade and migration paths listed below are virtual-to-virtual (V2V).

Table 3: Cisco Unified Communications Manager Releases Installed on Virtual Machines

From	To	Supported Method
8.6(x)	11.5(x)	Cisco Unified OS Admin PCD Migration or PCD Upgrade
9.x	11.5(x)	PCD Migration or PCD Upgrade
9.1(x)	11.5(x)	Cisco Unified OS Admin
10.x	11.5(x)	PCD Migration or PCD Upgrade
10.5(x)	11.5(x)	Cisco Unified OS Admin
11.0(1)	11.5(x)	Cisco Unified OS Admin PCD Migration or PCD Upgrade
11.5(x)	11.5(y)	Cisco Unified OS Admin PCD Migration or PCD Upgrade

Table 4: Cisco Unified Presence and IM and Presence Releases Installed on Virtual Machines

From	To	Supported Method
CUP 8.5(4)	11.5(x)	PCD Migration
CUP 8.6(3), 8.6(4), and 8.6(5)	11.5(x)	PCD Migration or PCD Upgrade

From	To	Supported Method
CUP 8.6(x)	11.5(x)	Cisco Unified OS Admin
IM and Presence 9.x	11.5(x)	PCD Migration or PCD Upgrade
IM and Presence 9.1(x)	11.5(x)	Cisco Unified OS Admin
IM and Presence 10.x	11.5(x)	PCD Migration or PCD Upgrade
IM and Presence 10.5(x)	11.5(x)	Cisco Unified OS Admin
IM and Presence 11.0(1)	11.5(x)	Cisco Unified OS Admin PCD Migration or PCD Upgrade
IM and Presence 11.5(x)	11.5(y)	Cisco Unified OS Admin PCD Migration or PCD Upgrade

COP Files Required for Upgrades to Release 11.5

The tables below lists the upgrade paths that require COP files. You must install COP files on each node before you begin an upgrade using the Cisco Unified OS Admin interface, or before you begin an upgrade or migration using the Prime Collaboration Deployment (PCD) tool. If you are using PCD, you can perform a bulk installation of the COP files before you begin the upgrade.

Table 5: Required COP Files for Upgrades and Migrations to Cisco Unified Communications Manager Release 11.5(x)

From	To	Upgrade Type
Releases prior to and including 8.5(x)	11.5(x)	Refresh upgrade. Required COP files: • ciscocm.refresh_upgrade_<latest_version>.cop.sgn • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
8.6(x)	11.5(x)	Refresh upgrade. Required COP files: • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn

From	To	Upgrade Type
9.1(x)	11.5(x)	Refresh upgrade. Required COP files: • ciscocm.version3-keys.cop.sgn Optional COP files: • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn) • ciscocm.free_common_space_v<latest_version>.cop.sgn
10.5(x)	11.5(x)	Standard upgrade; no COP file required.
11.0(x)	11.5(x)	Standard upgrade; no COP file required.
11.5(x)	11.5((y)	Standard upgrade; no COP file required.

Table 6: Required COP Files for Refresh Upgrades from Cisco Unified Presence Releases

From Cisco Unified Presence Release	To IM and Presence Release	Upgrade Type
8.5(4) through 8.6(1)	11.5(x)	Refresh upgrade. Requires the following COP files: • cisco.com.cup.refresh_upgrade_v<latest_version>.cop • ciscocm.version3-keys.cop.sgn

Table 7: Required COP Files for Refresh Upgrades from IM and Presence Service Releases

From IM and Presence Release	To IM and Presence Release	Upgrade Type
9.1(x)	11.5(x)	Refresh upgrade. Requires the following COP file: • ciscocm.version3-keys.cop.sgn
10.5(x)	11.5(x)	Standard upgrade; no COP file required.
11.0(x)	11.5(x)	Standard upgrade; no COP file required.
11.5(x)	11.5(y)	Standard upgrade; no COP file required.

Rolling Back to Previous Versions

If you run into any upgrade issues and you need to roll back to a previous version, you must roll back both the Cisco Unified Communications Manager and the IM and Presence Service installations to the previous version or you will have a non-supported version mismatch.

It's not supported to roll back the Cisco Unified Communications Manager version and leave the IM and Presence Service version at 11.5(1)SU2. Similarly, it's not supported to roll back the IM and Presence Service version and leave the Cisco Unified Communications Manager version at 11.5(1)SU2.

Upgrading with FIPS Mode Enabled

For Release 11.5(x), Cisco Unified Communications Manager and IM and Presence Service do not support RSA certificates with key-sizes that are less than 2048 bits when FIPS mode is enabled. This affects server certificates and LSCs.

If you are upgrading to Release 11.5(x) with FIPS mode enabled and you are using RSA key-sizes that are less than 2048 bits on your current version, then you can carry out one of the following items to resolve the problem.

You can either:

- Regenerate the effected certificates before you upgrade if your current version supports key-sizes of 2048 bits, or
- Regenerate the effected certificates after you upgrade to Release 11.5(x).

Note If you choose this option, then secure connections are not allowed to use the effected certificates until they have an RSA key-size of 2048 bits or greater.

Deprecated Phone Models

As of Cisco Unified Communications Manager Release 11.5, the following phones are no longer supported. If you use any of these phone models on an older release of Cisco Unified Communications Manager and you upgrade to Release 11.5, the phone will not work after the upgrade completes.

- Cisco IP Phone 12 S
- Cisco IP Phone 12 SP
- Cisco IP Phone 12 SP+
- Cisco IP Phone 30 SP+
- Cisco IP Phone 30 VIP
- Cisco Unified IP Phone 7902G
- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7910

- Cisco Unified IP Phone 7910G
- Cisco Unified IP Phone 7910+SW
- Cisco Unified IP Phone 7910G+SW
- Cisco Unified IP Phone 7912G
- Cisco Unified Wireless IP Phone 7920
- Cisco Unified IP Conference Station 7935

Upgrades that Involve Deprecated Phones

If you are using any of these phones on an earlier release and you want to upgrade to this release, do the following:

1. Confirm whether the phones in your network will be supported in Release 11.5.
2. Identify any non-supported phones.
3. For any non-supported phones, power down the phone and disconnect the phone from the network.
4. Provision a supported phone for the phone user. You can use the Migration FX tool to migrate from older model to newer model phones. For details, go to: http://refreshcollab.cisco.com/webportal/46/CUCM%20Readiness%20Assessment#endpoint_refresh_tool.
5. Once all the phones in your network are supported by Release 11.5, upgrade your system.

Note Deprecated phones can also be removed after the upgrade. When the administrator logs in to Cisco Unified Communications Manager after completing the upgrade, the system displays a warning message notifying the administrator of the deprecated phones.

Licensing

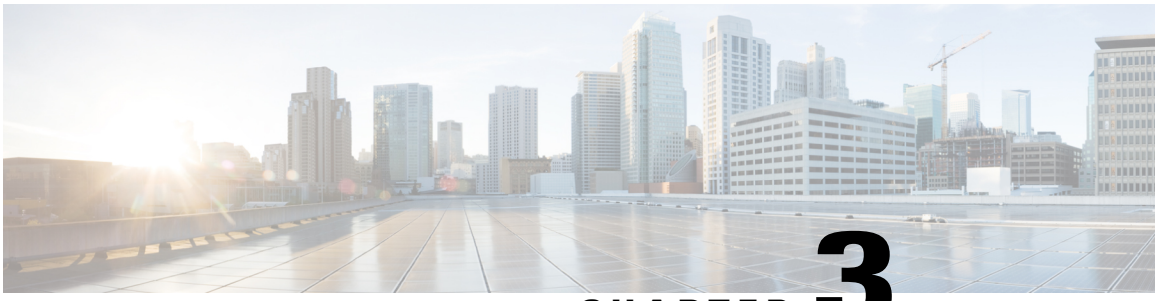
You do not need to purchase a new device license to replace a deprecated phone with a supported phone. The device license becomes available for a new phone when you either remove the deprecated phone from the system, or when you switch to the new Cisco Unified Communications Manager version, and the deprecated phone fails to register.

OS Admin Account Required for CLI-Initiated IM and Presence Upgrades

If you are using the **utils system upgrade** CLI command to upgrade IM and Presence Service nodes, you must use the default OS admin account, as opposed to a user with administrator privileges. Otherwise, the upgrade will not have the required privilege level to install essential services, thereby causing the upgrade to fail. You can confirm the account's privilege level by running the **show myself** CLI command. The account must have privilege level 4.

Please note that this limitation exists for CLI-initiated upgrades of IM and Presence Service only and does not apply to Cisco Unified Communications Manager. Also note that this limitation may be fixed for newer

ISO files. Refer to your ISO Readme file for details on your specific ISO file. For up to date information on this limitation, see CSCvb14399 at https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvb14399.



CHAPTER 3

New and Changed Features

- Cisco Meeting Server Conference Bridge, page 13
- Cisco Spark Remote Device, page 14
- Cisco Spark Remote Device Licensing, page 19
- Federation with Skype for Business, page 20
- IM and Presence Service Ad hoc Chat Room Discovery, page 20
- Log Compression for IM and Presence Service, page 20
- Push Notifications with Cisco Jabber for iPhone and iPad, page 21
- Rosters Cleanup for IM and Presence, page 26
- Persistent Chat High Availability , page 27
- MRA Support for Shared Line, page 28
- TLS as a Communication Protocol for Common Criteria Compliance, page 29

Cisco Meeting Server Conference Bridge

As of Release 11.5(1) SU2, Cisco Unified Communications Manager supports the Cisco Meeting Server conference bridge.

The Cisco Meeting Server conference bridge supports Ad Hoc, Meet-Me, Conference Now and Rendezvous conferences. This conference bridge offers premises-based audio, video, and web conferencing, and works with third-party on-premises infrastructure. It scales easily for small or large deployments. You can add capacity incrementally as needed, helping to ensure that you can support the current and future needs of your organization. This conference bridge provides advanced interoperability. Any number of participants can create and join meetings easily, from:

- Cisco or third-party room or desktop video systems
- Cisco Jabber Client
- Cisco Meeting App (can be native or with a WebRTC compatible browser)
- Skype for Business

A minimum release of Cisco Meeting Server 2.0 is required to use the Cisco Meeting Server conference bridge.

User Interface Updates

A new conference bridge type,**Cisco Meeting Server**, has been added to the **Conference Bridge configuration** window in Cisco Unified Communications Manager.

A new Normalization script **cisco-meeting-server-interop** has been added to provide interoperability between Cisco Unified Communications Manager and Cisco Meeting Server. This Normalization script configures a SIP trunk connection with Cisco Meeting Server.

For details on how to add a conference bridge in Cisco Unified Communications Manager, see the *Configure Conference Bridges* chapter of the *System Configuration Guide for Cisco Unified Communications Manager*.

Cisco Spark Remote Device

The Cisco Spark remote device is supported only for connecting your on-premises environment to Cisco cloud services. Use of this remote device for any other purpose is not supported. The following sections describe the new Cisco Spark remote device feature that is added as part of Cisco Unified Communications Manager Release, 11.5(1)su2.

Configure a Cisco Spark Remote Device

Procedure

	Command or Action	Purpose
Step 1	Configure a Cisco Spark Remote Device, on page 14	Create a Cisco Spark remote device.
Step 2	Add a Directory Number to a Cisco Spark Device, on page 19	To register a Cisco Spark remote device, you must add a Directory Number to that device.

Configure a Cisco Spark Remote Device

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Add New**.

Step 3 From the **Phone Type** drop down list, select Cisco Spark Remote Device and click **Next**.

Step 4 Configure the fields in the **Phone Configuration** window. See the Related Topics section for more information about the fields and their configuration options.

Step 5 Click **Save**.

What to Do Next

Related Topics

Cisco Spark Remote Device Configuration Fields, on page 15

Cisco Spark Remote Device Configuration Fields

Table 8: Cisco Spark Remote Device Configuration Fields

Field	Description
Device Information	
Registration	Specifies the registration status of the Cisco Spark remote device.
Device Status	Specifies if the device is active or inactive.
Device Trust	Specifies whether the device is trusted or not trusted.
Active Remote Destination	Specifies if the remote destination is active. The Cisco Spark client has only one active remote destination by default. All incoming calls are routed to the active remote destination. This field is to none even though it is associated to an active remote destination.
Owner User ID	From the drop-down list, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device.
Device Name	Specifies the name for the Cisco Spark remote device that is automatically populated based on the Owner User ID. The format of the device name is *SparkRD<OwnerUserID>* by default. The default device name *SparkRD* must not be changed. This field is editable. The device name can comprise up to 15 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.

Field	Description
Description	Enter a text description of the Cisco Spark remote device. This field can contain up to 128 characters. You can use all characters except quotes (“), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool	Select the device pool which defines the common characteristics for Cisco Spark remote devices. For more information on how to configure the device pool, see Device Pool Configuration Settings.
Calling Search Space	From the drop-down list, choose the calling search space or leave the calling search space as the default of <None>.
User Hold MOH Audio Source	From the drop-down list, choose the audio source to use for music on hold (MOH) when you initiate a hold action. **Caution** MOH is currently not supported for Cisco Spark remote device as Hold/Resume feature on the device is not implemented.
Network Hold MOH Audio Source	From the drop-down list, choose the audio source to use for MOH when the network initiates a hold action. **Caution** MOH is currently not supported for Cisco Spark remote device as Hold/Resume feature on the device is not implemented.
Location	From the drop-down list, choose the location that is associated with the phones and gateways in the device pool.
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device pool.
Ignore Presentation Indicators (internal calls only)	Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified CM ignores any presentation restriction that is received for internal calls.
Call Routing Information	
Inbound and Outbound Calls Information	

Field	Description
Calling Party Transformation CSS	This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.
Use Device Pool Calling Party Transformation CSS	To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the **Trunk Configuration** window.
Protocol Specific Information	
Presence Group	Configure this field with the Presence feature. If you are not using this application user with presence, leave the default (None) setting for presence group. From the drop-down list, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor. **Caution** Presence Group is currently not supported for Cisco Spark remote device .

Field	Description
SUBSCRIBE Calling Search Space	Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you can configure a calling search space as you do all calling search spaces. **Caution** SUBSCRIBE Calling Search Space is currently not supported for Cisco Spark remote device .
Rerouting Calling Search Space	From the drop-down list, choose a calling search space to use for rerouting. The rerouting calling search space of the referrer is used to find the route to the refer-to target. When the Refer message fails due to the rerouting calling search space, the Refer Primitive rejects the request with the "405 Method Not Allowed" message. The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.
Do Not Disturb Information	
Do Not Disturb	Check this check box to enable Do Not Disturb on the remote device. **Caution** The calls are not routed to Cisco Spark clients if the DND option is enabled. **Caution** Do Not Disturb is currently not supported for Cisco Spark remote device .

Field	Description
DND Option	When you enable DND on the phone, Call Reject option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call. **Caution** Do Not Disturb is currently not supported for Cisco Spark remote device .

Add a Directory Number to a Cisco Spark Device

To register a Cisco Spark remote device, add a Directory Number to that device. You cannot register a Cisco Spark remote device without a Directory Number. You can add a maximum of five Directory Numbers to the Cisco Spark remote device.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Specify the filter criteria and click the Cisco Spark Remote Device for which you want to associate the directory number.

Step 3 In the **Association** pane, click **Add a new DN** link.

Step 4 Configure the fields in the **Directory Number Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 Click **Save**.

Cisco Spark Remote Device Licensing

Starting with Release 11.5(1), users who do not have a licensed IP phone or TelePresence device, and who want to use the Cisco Spark remote device must purchase an enhanced license to use Spark. Each Spark license that is purchased gets added to the system license counts and appears in the License Usage Report.

A Cisco Spark remote device requires an enhanced license, except in the following scenario:

- When the Owner User ID for the Cisco Spark remote device is also assigned an IP Phone or Jabber client, a single enhanced license is used for both devices.
- When the Owner User ID for the Cisco Spark remote device is also assigned a Telepresence device, a single Telepresence license is used for both devices.

Federation with Skype for Business

Release 11.5(1)SU2 of the IM and Presence Service supports federation with Microsoft Skype for Business Server 2015 as follows:

- Interdomain Federation—Supports chat-only services via Expressway.
- Intradomain Federation—Supports chat-only services.

For details on how to configure interdomain or intradomain federation with Skype for Business, refer to the *Interdomain Federation for IM and Presence Service, Release 11.5(1)SU2* or the *Partitioned Intradomain Federation for IM and Presence Service Release 11.5(1)SU2* guides at the following URL:

http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html

IM and Presence Service Ad hoc Chat Room Discovery

A user can search for ad hoc chat rooms on a third-party client, but now they can only discover ad hoc chat rooms for which they are the owner or an administrator.

Note For users searching for chat rooms across intercluster connections, search results discover ad hoc chat rooms from clusters older than release 11.5(1), but not from clusters for this release or greater. Ad hoc chat rooms on release 11.5(1) clusters or greater can only be discovered by the owner or administrator of those chat rooms.

Log Compression for IM and Presence Service

This release introduces trace log file compression with gzip for many IM and Presence services. For each service that includes file compression, the maximum file size that you can assign for a log file has increased from 2 MB to 10 MB.

This update improves your ability to maintain and troubleshoot your system by allowing you to store more logs than ever before. For example, the maximum file size per log for the Cisco XCP Router service is changed from 2 MB to 10 MB, a 500% increase in the total log size allowance for that service.

In addition to the increased capacities, the default values for trace output has been updated in Cisco Unified IM and Presence Serviceability for each of the impacted services.

The following table summarizes the new limits and the new default values for the **Maximum No. of Files** and the **Maximum File Size (MB)** fields in the **Trace Configuration** window for each service that includes file compression. All log output files must be unzipped before they can be used.

Table 9: IM and Presence Service Trace Logs that Include File Compression

Service	Max # of Files Setting	Maximum File Size Setting	Log Output File Location
Cisco XCP Authentication Service	10,000 (limit) 500 (default)	10 MB (limit) 5 MB (default)	/epas/trace/xcp/log/auth-svc-1*.log.gz
Cisco XCP Connection Manager	10,000 (limit) 500 (default)	10 MB (limit and default)	/epas/trace/xcp/log/client-cm-1*.log.gz
Cisco XCP Router	10,000 (limit) 500 (default)	10 MB (limit and default)	/epas/trace/xcp/log/rtr-jsm-1*.log.gz
Cisco XCP Text Conference Manager	10,000 (limit) 500 (default)	10 MB (limit) 5 MB (default)	/epas/trace/xcp/log/txt-conf-1*.log.gz
Cisco Presence Engine	10,000 (limit) 250 (default)	10 MB (limit and default)	/epas/trace/epe/sdi/epe*.txt.gz
Cisco SIP Proxy	10,000 (limit) 250 (default)	10 MB (limit and default)	/epas/trace/esp/sdi/esp*.txt.gz
Cisco Config Agent	10,000 (limit) 250 (default)	10 MB (limit and default)	/epas/trace/epasca/sdi/epasca*.txt.gz
Cisco Presence Datastore	10,000 (limit) 250 (default)	10 MB (limit and default)	/epas/trace/imdb/sdi/ttsoft*.log.gz
Cisco Login Datastore	10,000 (limit) 250 (default)	10 MB (limit and default)	/epas/trace/imdb/sdi/ttlogin*.log.gz

Push Notifications with Cisco Jabber for iPhone and iPad

When your cluster is enabled for Push Notifications, the IM and Presence Service uses Apple's cloud-based Push Notification service to push instant message notifications to Cisco Jabber for iPhone and iPad clients that are running in the background. Enable Push Notifications in Cisco Unified Communications Manager to maintain a persistent instant messaging channel to Cisco Jabber. Push Notifications is required both for Cisco Jabber for iPhone and iPad clients that connect from within the enterprise network, and for clients that register to an on-premises IM and Presence Service via Expressway's Mobile and Remote Access (MRA) feature.

Note Push Notifications is required only for Cisco Jabber for iPhone and iPad clients. Android and Windows users are unaffected.

For details on how to configure the Push Notifications feature in the IM and Presence Service, see the "Push Notifications (On-Premises Deployments)" chapter of *Deploying Push Notifications for Cisco Jabber on iPhone and iPad in the IM and Presence Service and WebEx Messenger* at:

http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-configuration-examples-list.html

Note Push Notifications is also required for cloud deployments of Cisco Jabber for iPhone and iPad with WebEx Messenger. For details, see the "Push Notifications (Cloud Deployments)" chapter at the above document.

Performance Counters for Push Notifications

The following table shows the counters that have been added to the Cisco Unified Real Time Monitoring Tool to support Push Notifications for on-premises deployments of Cisco Unified Communications Manager and IM and Presence Service. Note that the counters increment only for specific APNS subscriber services (for example, APNS, APNS:beta, APNS:dev, APNS:test, APNS:load). For example, if the subscriber service is 'APNS:beta' only the APNS:beta counters increment, and none of the APNS:dev counters increment. The Cisco Jabber service type determines which subscriber service is used.

RTMT Counter	Counter Description	Counter increments if the Subscriber service is set to...
Cisco XCP Config Manager Counters		
NumberOfPushSuccess	Number of successful Push Notifications sent.	Any APNS Subscriber Services: • APNS • APNS:beta • APNS:dev • APNS:load • APNS:test
NumberOfPushFailure	Number of failed attempts to send Push Notifications.	
TargetInvalid	Total number of Push Notification failures due to an invalid target.	
TargetExpired	Total number of Push Notification failures due to an expired target.	
Cisco XCP Push Counters		

RTMT Counter	Counter Description	Counter increments if the Subscriber service is set to...
PushEnabledSessionsApns	Number of push enabled sessions for APNS clients with APNS as the subscriber service. The counter gets incremented when push notifications is enabled and decrements when push notifications is disabled or a session terminates.	APNS
PushEnableReqRcvdApns	Number of push enable requests received for clients with APNS as the subscriber service, during the 60 second interval. This counter resets to 0 every 60 seconds.	
PushErrorsApns	Number of push errors received during the 60 second interval. This counter resets to 0 every 60 seconds.	
PushSentSilentApns	Number of messages sent to sessions in silent mode during the 60 second interval. This counter resets to 0 every 60 seconds.	
PushSentDisconnApns	Number of messages sent to sessions in suspended state during the 60 second interval. This counter resets to 0 every 60 seconds.	
PushEnabledSessionsApnsBeta	Number of push enabled sessions for clients with APNS:beta as the subscriber service. The counter gets incremented when push notifications is enabled and decrements when push notifications is disabled or a session terminates.	APNS:beta
PushEnableReqRcvdApnsBeta	Number of push enable requests received for clients with APNS:beta as the subscriber service, during the 60 second interval. This counter resets to 0 every 60 seconds.	
PushErrorsApnsBeta	Number of push errors received during the 60 second interval where the subscriber service is APNS:beta. This counter resets to 0 every 60 seconds.	
PushSentSilentApnsBeta	Number of messages sent to sessions in silent mode during the 60 second interval where the subscriber service is APNS:beta. This counter resets to 0 every 60 seconds.	
PushSentDisconnApnsBeta	Number of messages sent to sessions in suspended state during the 60 second interval where the subscriber service is APNS:beta. This counter resets to 0 every 60 seconds.	

RTMT Counter	Counter Description	Counter increments if the Subscriber service is set to...
PushEnabledSessionsApnsDev	Number of push enabled sessions for clients with APNS:dev as the subscriber service. The counter gets incremented when push notifications is enabled and decrements when push notifications is disabled or a session terminates.	APNS:dev
PushEnableReqRcvdApnsDev	Number of push enable requests received for clients with APNS:dev as the subscriber service, during the 60 second interval. This counter resets to 0 every 60 seconds.	
PushErrorsApnsDev	Number of push errors received during the 60 second interval where the subscriber service is APNS:dev. This counter resets to 0 every 60 seconds.	
PushSentSilentApnsDev	Number of messages sent to sessions in silent mode during the 60 second interval where the subscriber service is APNS:dev. This counter resets to 0 every 60 seconds.	
PushSentDisconnApnsDev	Number of messages sent to sessions in suspended state during the 60 second interval where the subscriber service is APNS:dev. This counter resets to 0 every 60 seconds.	

RTMT Counter	Counter Description	Counter increments if the Subscriber service is set to...
PushEnabledSessionsApnsLoad	Number of push enabled sessions for clients with APNS:load as the subscriber service. The counter gets incremented when push notifications is enabled and decrements when push notifications is disabled or a session terminates;	APNS:load
PushEnableReqRcvdApnsLoad	Number of push enable requests received for clients with APNS:load as the subscriber service, during the 60 second interval. This counter resets to 0 every 60 seconds.	
PushErrorsApnsLoad	Number of push errors received during the 60 second interval where the subscriber service is APNS:load. This counter resets to 0 every 60 seconds.	
PushSentSilentApnsLoad	Number of messages sent to sessions in silent mode during the 60 second interval where the subscriber service is APNS:load. This counter resets to 0 every 60 seconds.	
PushSentDisconnApnsLoad	Number of messages sent to sessions in suspended state during the 60 second interval where the subscriber service is APNS:load. This counter resets to 0 every 60 seconds.	

RTMT Counter	Counter Description	Counter increments if the Subscriber service is set to...
PushEnabledSessionsApnsTest	Number of push enabled sessions for clients with APNS:test as the subscriber service. The counter gets incremented when push notifications is enabled and decrements when push notifications is disabled or a session terminates.	APNS:test
PushEnableReqRcvdApnsTest	Number of push enable requests received for clients with APNS:test as the subscriber service, during the 60 second interval. This counter resets to 0 every 60 seconds.	
PushErrorsApnsTest	Number of push errors received during the 60 second interval where the subscriber service is APNS:test. This counter resets to 0 every 60 seconds.	
PushSentSilentApnsTest	Number of messages sent to sessions in silent mode during the 60 second interval where the subscriber service is APNS:test. This counter resets to 0 every 60 seconds.	
PushSentDisconnApnsTest	Number of messages sent to sessions in suspended state during the 60 second interval where the subscriber service is APNS:test. This counter resets to 0 every 60 seconds.	

Rosters Cleanup for IM and Presence

With this release, the **utils rosters** set of CLI commands have been added to the IM and Presence Service. These commands help you to maintain system performance by allowing you to view and delete expired contacts and watchers from your system.

As employees leave your company, the database maintains those employees' contacts and watchers records. Over time, those records accumulate, and can begin to drain your system performance. With these new CLI commands you can quickly view and delete expired records, thereby keeping your system running at an optimal performance.

New utils rosters* CLI Commands

To support this feature, the following CLI commands have been added:

- **utils rosters list limited—**This command lists the count of invalid watchers and contacts.
- **utils rosters list full—**This command writes the details of all invalid watchers and contacts in a file and shows the total count on CLI.
- **utils rosters list watchers—**This command writes the details of all invalid watchers in a file and shows the count on CLI.

- **utils rosters list contacts—**This command writes the details of all invalid contacts in a file and shows the count on CLI.
- **utils rosters delete —**This command deletes all invalid watchers and invalid contacts that are present in the cluster.

Delete Invalid Contacts and Watchers

Use this procedure to delete invalid contacts and watchers from the database. If your system is running slow, one reason may be invalid contacts and watchers for employees who have left the company. The system maintains these records even after an employee leaves the company. Over time, invalid records for departed employees can accumulate and drag down system performance.

Complete the following procedure on the database publisher node:

Note We recommend that you complete this task only during a maintenance window.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils rosters list limited** CLI command to obtain a count of the total number of invalid watchers and contacts in the cluster.

Step 3 Optional. To write a detailed file with the full list of expired contacts and invalid watchers, run one of these commands:

- **utils rosters full—**Outputs a file with the invalid watchers and contacts in the cluster.
- **utils rosters list watchers—**Outputs a file with the invalid watchers in the cluster.
- **utils rosters list contacts—**Outputs a file with the invalid contacts in the cluster.

Step 4 Run the **utils rosters delete** command to delete invalid watchers and contacts.

Persistent Chat High Availability

From this release, you can now deploy the Persistent Chat High Availability feature with a Microsoft SQL Server (MSSQL) external database. Previously, MSSQL was not a supported database for Persistent Chat High Availability. In the event of IM and Presence Service node failure or Text Conferencing (TC) service failure, all persistent chat rooms hosted by that service are automatically hosted by the backup node TC service. After failover Jabber clients can seamlessly continue to use the persistent chat rooms.

Note Before configuring Persistent Chat Server for high availability, you should have one dedicated database instance located in the same physical data center in which the home front end of the Persistent Chat Server service is located. This database will serve as the SQL Server mirror for the primary Persistent Chat database. Optionally, designate an additional SQL Server to serve as the mirroring witness if you want an automated failover to the mirror database.

For additional information, see the "Persistent Chat High Availability" chapter of the *Configuration and Administration Guide for IM and Presence Service*.

MRA Support for Shared Line

Mobile and Remote Access (MRA) endpoints that register to Cisco Unified Communications Manager via Expressway now support shared lines. To use this feature, you must be running minimum releases of Cisco Unified Communications Manager, Release 11.5(1)SU2 and Expressway X8.9.

Cisco IP Phone 78xx and 88xx series now support this feature.

This feature is dependent on route path header support, which you must enable in Expressway. For configuration details, see the *Mobile and Remote Access via Cisco Expressway Deployment Guide, Release X8.9*.

Feature Limitations For MRA Endpoints

The following table summarizes feature limitations that were observed during the testing of Mobile and Remote Access (MRA)TelePresence and Jabber endpoints in deployments that interoperate Cisco Unified Communications Manager Release 11.5(1)SU2 with Expressway X8.9.

The testing on which this data is based covers the most commonly used features. However, it is not possible to test all scenarios, and as such, Cisco cannot guarantee support for all Cisco Unified Communications Manager features when interoperating with Expressway.

Feature	Feature Limitations
Shared Line	Supported by Cisco IP Phone 78xx and 88xx series. Not supported by other endpoints.
Hold/Resume	Audio failure may occur after a held call is resumed in the following cases: • Remote Jabber client calls remote TelePresence endpoint. • Remote TelePresence endpoint calls a TelePresence endpoint within the enterprise network.
Mobility calls	The following Mobility restrictions apply for remote endpoints: • Session handoff not supported • Dial via office reverse is not supported. Dial via office forward is supported.

Feature	Feature Limitations
Conferencing	The following restrictions apply for conferencing: • For conferences that include remote participants, the remote participant cannot be dropped from an active conference. • MeetMe conferencing is not supported with Cisco Jabber over MRA.
Call Park	Not supported
Call Pickup	Not supported
Call Monitoring	Not supported
Call Recording	Not supported
Call Preservation	Not supported
Extension Mobility	Supported with TelePresence endpoints. Not supported with Cisco Jabber.
Multistreaming	The ability of endpoints to negotiate multiple codecs in the audio channel is not supported.
Video codec support	H.265 is not supported.
Graceful registration	Not supported.
Roaming	Not supported
Called/Calling Party Transformation CSS	Not supported

TLS as a Communication Protocol for Common Criteria Compliance

As of Release 11.5(1) SU2, Transport Layer Security (TLS) 1.2 can be used as a communication protocol for syslog and FileBeat. This enables Cisco Unified Communications Manager and IM and Presence Service to comply with Common Criteria guidelines. The TLS 1.2 protocol enables the establishment of a secure connection in the following scenarios:

- Connecting Cisco Unified Communications Manager and IM and Presence Service with syslog servers
- Connecting FileBeat client with external logstash servers

Administrators can configure TLS for remote syslog and FileBeat using CLI commands.

Note Ensure that the syslog server supports TLS 1.2 protocol as a secure connection will be established only if the syslog server supports TLS 1.2 protocol.

New CLI Commands for Protocol Switch

Administrators with privilege level 4 access can configure TLS as the communication protocol using the following CLI commands:

- CLI command for remote syslog communication:

  `utils remotesyslog set protocol tls`- Sets TLS as the communication protocol for connecting Cisco Unified Communications Manager and IM and Presence Service with syslog servers

- CLI commands for FileBeat clients:

  - `utils filebeat tls enable`- Enables a secure connection between the FileBeat client and the logstash server.
  - `utils filebeat tls disable`- Disables the TLS for FileBeat client.
  - `utils filebeat tls status`- Displays the status for TLS.

New Alarms to Indicate Loss of Connection

An alarm `TLSRemoteSyslogDeliveryFailed` with severity `ERROR_ALARM` triggers if the connection between Cisco Unified Communications Manager or IM and Presence Service with syslog servers is lost. An alert Cisco `TLSRemoteSyslogDeliveryFailed` is also sent to RTMT Alert Central.