New and Changed Features

Authenticated Network Time Protocol Support

With this release, the authenticated Network Time Protocol (NTP) capability for Cisco Unified Communications Manager is supported. This support is added to secure the NTP server connection to Cisco Unified Communications Manager. In the previous releases, the Cisco Unified Communications Manager connection to the NTP server was not secure.

This feature is based on symmetric key-based authentication and is supported by NTPv3 and NTPv4 servers. Cisco Unified Communications Manager supports only SHA1-based encryption. The SHA1-based symmetric key support is available from NTP version 4.2.6 and above.

- Symmetric Key
- No Authentication

You can check the authentication status of the NTP servers through administration CLI or **NTP Server List** page of the **Cisco Unified OS Administration** application.

CLI Updates for Authenticated NTP

For the authenticated NTP support feature, the following new CLI command is added for this release:

- `utils ntp auth symmetric-key`—This command helps you enable or disable authentication of the selected NTP server. The authentication is based on symmetric keyID and key. The symmetric key is stored in the encrypted format in Cisco UnifiedCommunications Manager.

OS Administration Online Help Updates

Following column has been added in the **NTP Server List** page of the Cisco Unified Operating System Administration application.

NTP Servers Settings

Table 1: NTP Server Configuration Settings

Field	Description
NTP Authentication Status	Displays the authentication status of an NTP server.

Cisco Spark Remote Device

The Cisco Spark Remote Device (Cisco Spark-RD) is a dedicated and fully compatible virtual device for Hybrid Calling's functional requirements and behaviors. Cisco Spark-RD provides the following features:

- Remote Destination (Cisco Webex SIP address) length can be greater than 48 characters.
- Does not require an MTP for calls.
- Does not require IOS-MTP passthrough for video or screen share capability.
- A standalone Cisco Spark-RD uses one Enhanced UCL. If a user has any other UC device that requires an Enhanced UCL, then Cisco Spark-RD does not count towards the license total.

For more information about Cisco Spark-RDs and supported configuration for Hybrid Calling, see http://www.cisco.com/go/hybrid-services-call.

Calendar Integration with Office 365

With this release, you can integrate the IM and Presence Service with an Office 365 server for Microsoft Outlook calendar integration. This configuration allows the IM and Presence Service to pull user calendar information from an Office 365-hosted Microsoft Outlook and display it as a part of a user's presence status. If the user's Outlook calendar indicates that the user is in a meeting, that status gets pulled through and displays in the user's presence status.

This integration has been tested successfully with 15,000 IM and Presence users system, where 5,000 users have a meeting at the top of the hour.

For configuration details, refer to the document *Microsoft Outlook Calendar Integration with the IM and Presence Service*.

User Interface Updates

To support this feature, the **Presence Gateway Settings** window has been updated as follows

- The **Presence Gateway Type** field includes a new gateway option: **Office 365 Server**.
- The following HTTP Proxy fields are added: (**HTTP Proxy URL**, **HTTP Proxy Username**, and **HTTP Proxy Password**). An HTTP Proxy is required if the IM and Presence Service can't access the Office 365 server directly.

New Service Parameter

A new service parameter, **Office365 Calendar Information Pull Interval**, has been added for configuring the PULL interval with an Office 365 server. The IM and Presence Service is not currently able to pull calender information on an ad hoc basis. It can only pull calendar information at regularly scheduled intervals, as configured with this service parameter, which has a default setting of 60 minutes. Make sure to schedule an interval that meets your deployment needs.

Calendaring Troubleshooter

The Calendaring Troubleshooter portion of the System Troubleshooter (**Diagnostics** > **System Troubleshooter**) has been updated for Office 365 integration. When the IM and Presence Service is integrating with an Office 365 server, the troubleshooter confirms that the presence gateway is properly configured, and is reachable.

Cisco Jabber Authentication via OAuth Refresh Logins

Cisco Jabber clients, as of Jabber Release 11.9, can use OAuth Refresh Logins to authenticate with Cisco Unified Communications Manager and the IM and Presence Service. This feature improves the user experience for Cisco Jabber by providing the following benefits:

- After an initial login, provides seamless access to resources over the life of the refresh token.
- Removes the need for Cisco Jabber clients to re-authenticate frequently.
- Provides consistent login behavior in SSO and non-SSO environments.

With OAuth Refresh Logins, Cisco Unified Communications Manager issues clusterwide access tokens and refresh tokens that use the OAuth standard. Cisco Unified Communications Manager and IM and Presence Service use the short-lived access tokens to authenticate Jabber (the default lifespan for an access token is 60 minutes). The longer-lived refresh tokens provide Jabber with new access tokens as the old access tokens expire. So long as the refresh token is valid the Jabber client can obtain new access tokens dynamically without the user having to re-enter credentials (the default refresh token lifespan is 60 days).

All access tokens are encrypted, signed, and self-contained using the JWT format (RFC7519). Refresh tokens are signed, but are not encrypted.

Note OAuth authentication is also supported by Cisco Expressway and Cisco Unified Connection. Make sure to check with those products for compatible versions. Refer to Cisco Jabber documentation for details on Jabber behavior if you are running incompatible versions.

Authentication Process

When a Cisco Jabber client authenticates, or when a refresh token is sent, Cisco Unified Communications Manager checks the following conditions, each of which must be met for authentication to succeed.

- Verifies the signature.
- Decrypts and verifies the token.
- Verifies that the user is an active user. For example, an LDAP-synced user whom is subsequently removed from the external LDAP directory, will remain in the database, but will appear as an inactive user in the User Status of End User Configuration.
- Verifies that the user has access to resources, as provided by their role, access control group, and user rank configuration.

Note For backward compatibility, older Jabber clients and supporting applications such as the Cisco Unified Real-Time Monitoring Tool can authenticate using the implicit grant flow model, which is enabled by default.

Enterprise Parameter Updates

To support this feature, the following enterprise parameters are added under the **SSO and OAuth Configuration** heading:

- **OAuth with Refresh Login Flow**—This parameter controls the login flow used by clients such as Jabber when connecting to Unified CM. OAuth with Refresh Login Flow "enabled" allows the client to use an oAuth-based Fast Login flow to provide a quicker and streamlined login experience, without requiring user input to re-log in (such as after a network change). The option requires support from the other components of the Unified Communications solution, such as Expressway and Unity Connection (compatible versions with refresh login flow enabled). The OAuth with Refresh Login Flow "disabled" option preserves existing behavior and is compatible with older versions of other system components. Note: For Mobile and Remote Access deployment with Jabber, It is recommended to enable this parameter only with a compatible version of Expressway which supports oAuth with Refresh login flow. Incompatible version may impact Jabber functionality. See the specific product documents for supported version and configuration requirements.
- **OAuth Refresh Token Expiry Timer (days)**— This parameter determines the OAuth Refresh token expiry timer in days. Updates to this parameter take effect immediately and refresh tokens issued after the change will use the new expiry timer and previously issued refresh tokens will cease to be valid.

Certificate Updates

To support this feature, the self-signed **AUTHZ** certificate has been added to handle authentication with OAuth tokens. This certificate lives on the Cisco Unified Communications Manager publisher node and replicates the signing and encryption keys to all Cisco Unified Communications Manager and IM and Presence Service cluster nodes. The certificate is self-signed, using a locally-generated public-private key pair and should not be an X.509 certificate.

If you think that either the signing key or encryption key has been compromised, you can regenerate either set of keys. Make sure to sync your new keys with Cisco Expressway and Cisco Unity Connection.

CLI Updates

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

- `set key regen authz signing`—Run this command on the Cisco Unified Communications Manager publisher node to regenerate the asymmetric RSA key pair for signing OAuth access tokens and refresh tokens.
- `set key regen authz encryption`—Run this command on the Cisco Unified Communications Manager publisher node to regenerate the symmetric encryption key that encrypts OAuth access tokens and refresh tokens.
- `show key authz signing`—This command displays the OAuth refresh login encryption key checksum and last synced time on both publisher and subscriber nodes.
- `show key authz encryption`—This command displays the OAuth refresh login signing key checksum and last synced time on both publisher and subscriber nodes.

Troubleshooting

The following table highlights useful logs for troubleshooting OAuth SSO configuration. Trace does not need to be configured for these logs.

Note To set SAML SSO logs to a detailed level, run the `set samltrace level debug` CLI command.

Table 2: Logs for Troubleshooting OAuth Refresh Logins

Logs	Log Details
SSO Logs	Each time a new SSO App operation is completed, new log entries are generated here: `/var/log/active/platform/log/ssoApp.log`
Ssosp Logs	SSO and OAuth operations are logged in ssosp logs. Each time SSO is enabled a new log file is created here: `/usr/local/thirdparty/Jakarta-tomcat/logs/ssosp/log4j/`
SSO and OAuth Configuration	Certificate logs are located at the following location. Each time the Authz certificate is regenerated, a new log file is generated: `/var/log/active/platform/log/certMgmt*.log`

Configure Refresh Logins for Cisco Jabber

Use this procedure to enable Refresh Logins with OAuth access tokens and refresh tokens in Unified Communications Manager. OAuth Refresh Logins provides a streamlined login flow that doesn't require users to re-login after network changes.

Note To ensure compatibility, make sure that the various Unified Communications components of your deployment, such as Cisco Jabber, Cisco Expressway and Cisco Unity Connection, support refresh logins. Once OAuth Refresh Logins are enabled, disabling the feature will require you to reset all Cisco Jabber clients.

Before you begin

You must be running a minimum release of Cisco Jabber 11.9. Older versions of Jabber will use the Implicit Grant Flow authentication model from previous releases.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Under **SSO Configuration**, do either of the following:

- Choose the **OAuth with Refresh Login Flow** enterprise parameter to **Enabled** to enable OAuth Refresh Logins.
- Choose the **OAuth with Refresh Login Flow** enterprise parameter to **Disabled** to disable OAuth Refresh Logins. This is the default setting.

Step 3 If you enabled OAuth Refresh Logins, configure expiry timers for access tokens and refresh tokens by configuring the following enterprise parameters:

- **OAuth Access Token Expiry Timer (minutes)**—This parameter specifies the expiry timer, in minutes, for individual OAuth access tokens. The OAuth access token is invalid after the timer expires, but the Jabber client can request and obtain new access tokens without the user having to re-authenticate so long as the refresh token is valid. The valid range is from 1 - 1440 minutes with a default of 60 minutes.
- **OAuth Refresh Token Expiry Timer (days)**—This parameter specifies the expiry timer, in days, for OAuth refresh tokens. After the timer expires, the refresh token becomes invalid and the Jabber client must re-authenticate to get a new refresh token. The valid range is from 1 - 365 days with a default of 60 days.

Step 4 Click **Save**.

Note Once you've saved the configuration, reset all Cisco Jabber and Webex clients.

Regenerate Keys for OAuth Refresh Logins

Use this procedure to regenerate both the encryption key and the signing key using the Command Line Interface. Complete this task only if the encryption key or signing key that Cisco Jabber uses for OAuth authentication with Unified Communications Manager has been compromised. The signing key is asymmetric and RSA-based whereas the encryption key is a symmetric key.

After you complete this task, the current access and refresh tokens that use these keys become invalid.

We recommend that you complete this task during off-hours to minimize the impact to end users.

The encryption key can be regenerated only via the CLI below, but you can also use the Cisco Unified OS Administration GUI of the publisher to regenerate the signing key. Choose **Security** > **Certificate Management**, select the**AUTHZ** certificate, and click **Regenerate**.

Procedure

Step 1 From the Unified Communications Manager publisher node, log in to the **Command Line** Interface .

Step 2 If you want to regenerate the encryption key:

a) Run the `set key regen authz encryption` command.

b) Enter `yes`.

Step 3 If you want to regenerate the signing key:

a) Run the `set key regen authz signing` command.

b) Enter `yes`.
The Unified Communications Manager publisher node regenerates keys and replicates the new keys to all Unified Communications Manager cluster nodes, including any local IM and Presence Service nodes.

You must regenerate and sync your new keys on all of your UC clusters:

- IM and Presence central cluster—If you have an IM and Presence centralized deployment, your IM and Presence nodes are running on a separate cluster from your telephony. In this case, repeat this procedure on the Unified Communications Manager publisher node of the IM and Presence Service central cluster.
- Cisco Expressway or Cisco Unity Connection—Regenerate the keys on those clusters as well. See your Cisco Expressway and Cisco Unity Connection documentation for details.

Revoke Existing OAuth Refresh Tokens

Use an AXL API to revoke existing OAuth refresh tokens. For example, if an employee leaves your company, you can use this API to revoke that employee's current refresh token so that they cannot obtain new access tokens and will no longer be able to log in to the company account. The API is a REST-based API that is protected by AXL credentials. You can use any command-line tool to invoke the API. The following command provides an example of a cURL command that can be used to revoke a refresh token:

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

where:

- `admin:password` is the login ID and password for the Cisco Unified Communications Manager administrator account.
- `UCMaddress` is the FQDN or IP address of the Cisco Unified Communications Manger publisher node.
- `end_user` is the user ID for the user for whom you want to revoke refresh tokens.

Compliance to Common Criteria

With Release 11.5(1) SU3, both Cisco Unified Communications Manager and IM and Presence Service can run in Common Criteria mode. This running mode runs on a FIPS-enabled system, and allows the system to comply with Common Criteria guidelines.

Common Criteria mode can be configured by running the following CLI commands on each cluster node:

- `utils fips_common_criteria enable` - Run this command to turn Common Criteria mode on.
- `utils fips_common_criteria disable` - Run this command to turn off Common Criteria mode.
- `utils fips_common_criteria status` - Run this command to confirm whether Common Criteria mode is on or off for a particular cluster node.

TLS connection between the MS SQL external database server and the IM and Presence Service server is not supported when Common Criteria mode is enabled on the IM and Presence Service server.

Emergency Notifications Paging

With this release, Cisco Unified Communications Manager comes with a provisioning wizard that allows you to quickly provision and configure advanced notification services.

The Cisco Paging Server product is offered through InformaCast Virtual Appliance. It is a software solution that transforms devices on your network into a powerful system for IP paging and emergency call alerting. It integrates easily with Cisco phones, overhead speakers, strobes, panic buttons, and more, to increase the speed, reach, and success rate of your emergency alerts.

User Interface Updates for Advanced Notification Services

In the **Advanced Features** menu of the Cisco Unified Communications Manager Administration, the **Emergency Notifications Paging** wizard has been added. **Emergency Notifications Paging** is a full-featured emergency notification and paging solution that allows you to reach an unlimited number of Cisco IP phones and various devices and systems with text and audio messages. It includes the following features:

- InformaCast advanced notification
- Panic button configuration
- Text and audio notification to IP phones when a user dials an emergency services number (CallAware)

For more information about InformaCast Virtual Appliance, see https://www.singlewire.com/informacast.html.

Advanced Notification Paging Configuration Task Flow

Perform the following tasks to integrate InformaCast Paging Server with Unified Communications Manager for IP paging and emergency call alerting. It includes the following features:

- InformaCast advanced notification
- Panic button configuration
- Text and audio notification to IP phones when a user dials an emergency services number (CallAware)

Procedure

	Command or Action	Purpose
Step 1	Install the InformaCast Virtual Appliance, on page 9.	Download the InformaCast OVA file from the Singlewire website and upload it to vSphere.
Step 2	Configure Connection to InformaCast, on page 11.	Configure Unified Communications Manager and InformaCast.
Step 3	Configure Panic Button, on page 12.	Configure a panic button to send a text and audio notification to IP phones.
Step 4	Configure CallAware Emergency Call Alerting, on page 13.	Configure emergency call text and audio notifications.

Install the InformaCast Virtual Appliance

Singlewire supports InformaCast Virtual Appliance on the VMware ESXi platform, which is managed through the vSphere client.

Note To view a list of Singlewire-supported VMware ESXi versions, go to this URL: https://www.singlewire.com/compatibility-matrix and click the Server Platforms link under InformaCast Platform section.

Note If you have purchased a license, refer to https://www.singlewire.com/icva-kb-activate to activate your license. This will ensure that Emergency Notifications stay active after the 90-day trial.

Note For more details on the installation, including InformaCast screen captures, go to this URL: https://www.singlewire.com/icva-kb-install.

Before you begin

Import InformaCast Virtual Appliance using the vSphere client. This can be downloaded from your VMware server.

Procedure

Step 1 Download the OVA file from the Singlewire website and then log in to the vSphere client.

Note If you are using InformaCast on the Communications Manager Business Edition 6000, you are supplied with a DVD in a package with an OVA on it (physical media).

The **vSphere Client** window appears.

Step 2 From the **vSphere Client** window, choose **File** > **Deploy OVF Template**.

The **Deploy OVF Template** dialog box appears.

Step 3 Click the **Deploy from File** radio button and then click **Browse** to select the saved the OVA file (or to the OVA file on the supplied DVD). After you select the OVA file, click **Open**.
The **Source** location is selected in the **Deploy OVF Template** dialog box.

Step 4 Click **Next** to continue.
The **Deploy OVF Template** dialog box refreshes and **OVF Template Details** appears.

Step 5 Click **Next** to verify the **Name and Location**, and then click **Next** to select the network to store the new virtual machine files.

Tip It is good practice to place the Virtual Appliance on the same VLAN as your Cisco Unified Communications Manager.

Step 6 Click **Next** to continue, and then click **Finish**.
The InformaCast Virtual Appliance begins importing.

Step 7 From the **vSphere Client** window, click **Hosts and Clusters** icon and then select your host server.
The **vSphere Client** window refreshes.

Step 8 Click the **Configuration** tab and select the **Virtual Machine Startup/Shutdown** link in the **Software** section.

Step 9 Click the **Properties** link.
The **Virtual Machine Startup and Shutdown** dialog box appears.

Step 10 Check the **Allow virtual machines to start and stop automatically with the system** check box under **System Settings**.

Step 11 Under **Startup Order**, scroll to the **Manual Startup** section and select your virtual machine (by default, this is Singlewire InformaCast VM), and then move it from the **Manual Startup** section to the **Automatic Startup** section, by using the **Move Up** button. After moving it, click **OK**.
The InformaCast Virtual Appliance starts and stops automatically with the server on which it is hosted. Now you can turn on InformaCast's virtual machine and set its network configuration.

Step 12 Choose **View** > **Inventory** > **VMs and Templates** and then select your virtual machine.

Step 13 Choose the **Inventory** > **Virtual Machine** > **Open Console**
The Singlewire InformaCast VM console window appears.

Step 14 InformaCast configuration starts for the first time. During this configuration, perform the following tasks for the InformaCast Virtual Appliance:

a) Accept Cisco End User License Agreement (EULA)
b) Accept Singlewire EULA
c) Set up hostname
d) Set up IP address, subnet mask, and default gateway
e) Set up DNS server IP address and domain name
f) Set up NTP server IP address or hostname
g) Set up time zone
h) Set up Secure Socket Layer (SSL) certificate parameters
i) Set up SSL subject alternate names (optional)
j) Set up the OS admin password
k) Set up the InformaCast and PTT (PushToTalk) admin password. This password is required to connect the Cisco Unified Communications Manager and InformaCast in the Cisco Unified CM Administration, **Advanced Features** > **Emergency Notifications Paging**.
l) Set up security passphrase for backup and communication

When your configuration is successful, the “Welcome to Singlewire InformaCast” message is displayed.

Step 15 Click **Continue** to work with Singlewire InformaCast.

Configure Connection to InformaCast

Use this procedure to load the InformaCast certificate to the Unified Communications Manager Tomcat trust store.

Before you begin

Install the InformaCast Virtual Appliance, on page 9.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **Emergency Notifications Paging**.

Step 2 In the **Introduction to InformaCast Emergency Notifications** page, click **Next** to continue.
The **Installing the InformaCast Virtual Appliance** page appears.

Step 3 In the **Installing the InformaCast Virtual Appliance** page, click **Next** to continue.

Note You should have successfully installed InformaCast Virtual Appliance to configure with the Unified Communications Manager.

The **Connecting Cisco Unified Communications Manager and InformaCast** page appears.

Step 4 In the **IP address of InformaCast VM** field, enter either IP address or Hostname.

Note By default, the username is stated as `admin` in the **Username to use in InformaCast** field, and it is not editable.

Step 5 In the **Password for admin app user** field, enter the administrator password of the InformaCast application.
The dialog box displaying the thumbprint of InformaCast certificate is displayed.

Step 6 Click **OK** to load the InformaCast certificate to the Unified Communications Manager Tomcat trust store.
Configuration process starts.

Note When the configuration is successful, the **Status** field displays the completion status.

Step 7 Click **Next**.
The wizard performs the following tasks:

- Activates SNMP service
- Configures SNMP Service with locally generated random credentials
- Activates CTI Manager Service
- Configures Unified Communications Manager for InformaCast
    - Creates new region (1 per cluster)
    - Creates new device pool (1 per cluster)
    - Creates SIP trunk (1 per cluster)
    - Creates route group (1 per cluster)

- Creates route list
- Creates role
- Creates app user

- Configures InformaCast for Unified Communications Manager
  - Creates a cluster
  - Refreshes recipient groups
  - Sets SIP access to deny
  - Creates SIP access

Configure Panic Button

Use this procedure to configure a panic button to send a text and audio notification to IP phones. This allows you to initiate a one click alarm if there is emergency.

Before you begin

Configure Connection to InformaCast, on page 11.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **Emergency Notifications Paging**.

Step 2 In the **Introduction to InformaCast Emergency Notifications** page, click **Next** to continue.

Step 3 In the **Installing the InformaCast Virtual Appliance** page, click **Next** to continue.

Step 4 In the **Connecting Cisco Unified Communications Manager and InformaCast** page, click **Next** to continue.
The **Configuring a Panic Button** page appears.

Step 5 From the **Choose pre-recorded message by name** drop-down list, select the pre-recorded message to be displayed on Cisco Unified IP phones and various devices and systems in emergency.

Note You can change the pre-recorded message in InformaCast administration, as required.

Step 6 In the **Enter DN to trigger the panic button** field, enter the Directory Number (DN), which includes the digits 0 to 9, asterisks (*), and pound signs (#). Default value is ***5.

Step 7 From the **Route Partition** drop-down list, select a partition to restrict access to the route pattern.

Note If you do not want to restrict access to the route pattern, select <None> for the partition.

Step 8 Click **Choose Phones to Send Notification** button.
The **Phones to Send Notification** dialog box appears.

Step 9 From the **Phones to Send Notification** dialog box, select the Cisco Unified IP phones to send the pre-recorded message. The dial pattern entered by you (for example, ***5) is configured as speed dial on the selected phones.
The selected Cisco Unified IP Phone are displayed in the **Selected Phones to Send Notification** list box.

Step 10 Click **Add Rules**, to create a new rule for the selected Cisco Unified IP Phone to receive notifications.

a) Select one of the parameters from the drop-down list. The available options are Device Pool, Description, and Directory Number.

b) In the second drop-down list, select a criteria from the following options:

- Does
- Does not

c) In the third drop-down list, select a criteria from the following options:

- Begins with
- Ends with
- Contains

d) In the text box, enter the search criterion.

Note Minimum of one new rule and maximum of new five rules can be created. The **Add Rules** button gets disabled when five rules are created.

Note To delete a rule, click **Delete Rules**.

e) Click **Test Rules**, to validate the created rules. When the test rule is completed with more than zero phones, the **Next** button is enabled.

Note Phones added to Cisco Unified Communications Manager at a later date that match this rule will be included as recipients in notifications to this group.

Step 11 Click **Next**.

The wizard performs the following tasks:

- Adds a speed dial for the entered DN to the selected phones. If the selected phones have unused speed dials assigned to existing phone button templates, this speed dial appears directly on the selected phones. If the selected phones do not have unused speed dial buttons, the panic button speed dial is created, but it does not appear on the phone.
- Adds route pattern for entered DN in selected partition using created route list.
- Creates an InformaCast DialCast entry for the entered DN to send the selected message to the phones matching the selected rules.

Configure CallAware Emergency Call Alerting

Use this procedure to configure the CallAware emergency call alerting details. This sends a text and audio notification to IP phones when an emergency number is dialed. It can also detect calls to numbers other than 911.

Before you begin

Configure Panic Button, on page 12.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **Emergency Notifications Paging**.

Step 2 In the **Introduction to InformaCast Emergency Notifications** page, click **Next** to continue.

Step 3 In the **Installing the InformaCast Virtual Appliance** page, click **Next** to continue.

Step 4 In the **Connecting Cisco Unified Communications Manager and InformaCast** page, click **Next** to continue.

Step 5 In the **Configuring a Panic Button** page, click **Next** to continue.
The **Configuring CallAware Emergency Call Alerting** page appears.

Step 6 From the **Choose pre-recorded message by name** drop-down list, select the pre-recorded message to be displayed on Cisco Unified IP phones and various devices and systems in emergency.

Note You can change the pre-recorded message in InformaCast administration, as required.

Step 7 Click **Choose Emergency Route Patterns** button.
The **Route Patterns** dialog box appears.

Step 8 From the **Route Patterns** dialog box, select the route patterns by checking the box next to the desired patterns.

a) Click the **Save Selected/Changes** button.

The selected route patterns are displayed in the **Selected Route Patterns** list box.

Step 9 Click **Add Rules**, to create a new rule for the selected Cisco Unified IP Phone to receive notifications.

a) Select one of the parameters from the drop-down list. The available options are Device Pool, Description, and Directory Number.

b) In the second drop-down list, select a criteria from the following options:

- Does
- Does not

c) In the third drop-down list, select a criteria from the following options:

- Begins with
- Ends with
- Contains

d) In the text box, enter the search criterion.

Note Minimum of one new rule and maximum of five new rules can be created. The **Add Rules** button gets disabled when five rules are created.

Note To delete a rule, click **Delete Rules**.

e) Click **Test Rules**, to validate the created rules. When the test rule is completed with more than zero phones, the **Finish** button is enabled.

Note Phones added to Unified Communications Manager at a later date that match this rule will be included as recipients in notifications to this group.

Step 10 Click **Finish**.

The wizard performs the following tasks:

- Adds External Call Control profile for InformaCast
- For each selected route pattern, modify that route pattern to reference the External Call Control profile
- Creates a recipient group with rules that match phones to receive the notification
- Creates an InformaCast routing request with the selected message and recipient group

The **Summary** page appears and confirms the successful configuration of InformaCast with Unified Communications Manager. For more information, see https://www.singlewire.com.

Paging Interactions

- Advanced Notification Paging Interactions, on page 15

Advanced Notification Paging Interactions

Table 3: Advanced Notification Paging Interactions

Feature	Interaction
Emergency Notifications Paging	You can configure the Emergency Notifications Paging wizard using InformaCast Release 11.5(1)SU3 and later versions in basic paging mode only. You can configure call monitoring to route patterns that contain digits only in the Emergency Notifications Paging wizard. For route patterns that contain wildcard characters, configure in InformaCast.

Encryption License Requirement for Mixed-Mode

This release of Cisco Unified Communications Manager introduces support for encryption licenses. If you want to enable mixed-mode in Cisco Unified Communications Manager, you must have an encryption license installed in Cisco Prime License Manager and applied against Cisco Unified Communications Manager.

Fresh Installations

Upon installing your cluster, you will be unable to move the cluster into mixed-mode unless you have an encryption license applied against Cisco Unified Communications Manager, and a sync has been completed. If you do not have an encryption license, and you attempt to move the cluster into mixed-mode, an empty CTL file will be generated and the cluster will remain in non-secure mode.

Upgrades

If you upgrade from an earlier release with mixed-mode enabled, but you do not have an encryption license installed, a warning message on the encryption license requirement displays on the user interface immediately following the upgrade. You will also receive the **CiscoSystemEncryptionNotAllowed** alert. Your system

will continue to operate in mixed-mode, but you will be unable to update the CTL file and will continue to receive this alert until you either install an encryption license or move the cluster security setting back to non-secure mode. Cisco recommends that you install the encryption license at the earliest to ensure that you can continue to run mixed mode without any disruption.

If you were not running mixed-mode prior to the upgrade, you will be unable to move the cluster into mixed-mode unless you have an encryption license applied against Cisco Unified Communications Manager, and a sync has been completed.

User Interface Updates

In the Cisco Unified CM Administration interface's **License Usage Report** window, a new field has been added to the **Cisco Prime License Manager** section:

- **Encryption License installed**—This field contains a **True** or **False** value that indicates whether an encryption license is installed.

Ordering and Installing License Files

The following table describes how to update your system with an encryption license.

Table 4: Updating your System with an Encryption License

Step	Task	Description
Step 1	Obtain an ENC PAK license file.	Use the CUCM-PLM-ENC-K9= part number to order encryption licenses via the Product Upgrade Tool at https://tools.cisco.com/gct/Upgrade/jsp/index.jsp. For further information on ordering licenses, see the Cisco Unified Communications Solutions Ordering Guide. **Note** If you are using multiple instances of Cisco Prime License Manager in your deployment, you must order a separate encryption license for each Prime License Manager instance.
Step 2	Install the encryption license file in Cisco Prime License Manager.	Follow the "Upgrade Existing Licenses" procedure in the Cisco Prime License Manager User Guide, Release 11.5(1)SU2.
Step 3	Synchronize licenses.	In Cisco Prime License Manager, select the **Product Instances** tab and click **Synchronize licenses**. For additional detail, see the *Cisco Prime License Manager User Guide, Release 11.5(1)SU2*.

Enhanced Sign-In Experience for Cisco Jabber During SSO and Non-SSO

From this release, the sign-in experience for Cisco Jabber will be similar for Single Sign-On (SSO) and non-SSO. The refresh token feature enhances the Jabber user experience across devices and especially for Jabber on Mobile. The login flow for Jabber non-SSO is now similar to Jabber SSO . An end user can now sign-in by generating an OAuth code, which in turn generates an access token and a refresh token to enable logging in to Jabber. When an access token expires, the refresh token is used to generate the access token. This prevents the login flow from being repeated and enhances performance during Jabber sign-in.

Cisco Jabber Client version 11.9.0 supports the refresh token feature.

Enhanced Usability in the User Device Association Screen

The **User Device Association** screen allows administrators to associate or disassociate devices with end users and application users. As of Release 115.1 SU3, the user interface of the **User Device Association** screen has been enhanced to ensure that an admin is sure about working on the selected user. The **Remove All Associated Devices** button has been realigned on the UI to prevent an admin from unintentionally removing devices associated with a user.

User Interface Updates

- The User ID of the selected user is displayed in the **User Device Association** screen. The following labels have been updated:
  - The name of the section **User Device Association** is now updated to **User Device Association For <User ID>**.
  - The name of the check box **Show the devices already associated** is now updated to **Show the devices already associated with <User ID>**.
- The **Remove All Associated Devices** button is now available at the right corner of the toolbar to distinguish it from other toolbar buttons.
- The confirmation message displayed on clicking the **Remove All Associated Devices** button now specifies the user ID and number of devices selected for disassociation.
- The **Remove All Associated Devices** button is not displayed when the filter is applied. This ensures that an admin does not unintentionally disassociate all the associated devices.

Minimum TLS Version Control

This release of Cisco Unified Communications Manager and IM and Presence Services includes the minimum Transport Layer Security (TLS) protocol version configuration support. Use this feature to configure the minimum TLS version to comply with the organization security policies.

The supported TLS versions are TLS 1.0, 1.1, and 1.2. By default, TLS 1.0 is configured. After you configure the minimum TLS version, both the minimum version and the higher versions are supported.

Before you configure the minimum TLS version, ensure that the following products support secure connection of the selected minimum TLS version configured or above with Cisco Unified Communications Manager and IM and Presence Services. If this requirement is not met, upgrade the product to a version that supports the interoperability for selected minimum TLS version configured or above when you configure the minimum TLS version.

- Skinny Client Control Protocol (SCCP) Conference Bridge
- Transcoder
- Hardware Media Termination Point (MTP)
- SIP Gateway
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment
- Cisco Unified Border Element (CUBE)
- Cisco Expressway
- Cisco TelePresence Conductor

Note

- This feature is implemented at Command Line Interface and is applicable to both Cisco Unified Communications Manager and IM and Presence Services.
- Cisco Unified Communications Manager and IM and Presence Services Release 9.x and below do not support TLS 1.1 and above. Hence, before you proceed for interoperability of these applications of Release 9.x with Cisco Unified Communications Manager and IM and Presence Services of Release 11.5(1)SU3 and above, configure minimum TLS version as 1.0. This configuration is required for functions, such as Extensible Messaging and Presence Protocol (XMPP) federation deployment, Extension Mobility Cross Cluster (EMCC), Inter Cluster Sync Agent (ICSA), and SIP Trunk functionality that do not support TLS 1.1 and above.
- You can enable Common Criteria mode along with configuration of minimum TLS version. If you do so, the applications continue to comply with Common Criteria requirements and disable TLS 1.0 secure connections at application level. When the common criteria mode is enabled, you can configure the minimum TLS version as either 1.1 or 1.2 for the applications. If you try to configure the minimum TLS version as 1.0, an error appears at Command Line Interface. For details on Common Criteria mode, see the Compliance to Common Criteria topic of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

To configure the minimum TLS version, see the CLI Commands for Minimum TLS Version, on page 18 topic.

CLI Commands for Minimum TLS Version

For the minimum TLS version feature, the following new CLI commands are added for this release:

- `set tls min-version`—This command sets the minimum version of Transport Layer Security (TLS) protocol.
- `show tls min-version`—This command shows the minimum configured version of Transport Layer Security (TLS) protocol.

For additional information on these CLI commands, see 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.

Security Guide Updates

The new chapter, "TLS Setup", is added to the *Security Guide for Cisco Unified Communications Manager*. The chapter is added to include the Minimum TLS Version Control feature that is introduced with this release. The chapter provides an overview of TLS, its prerequisites, how to configure TLS, and the interactions and restrictions.

TLS Overview

Transport Layer Security (TLS) provides secure and reliable signaling and data transfer between two systems or devices, by using secure ports and certificate exchange. TLS secures and controls connections among Unified Communications Manager-controlled systems, devices, and processes to prevent access to the voice domain.

TLS Prerequisites

Before you configure the minimum TLS version, make sure that your network devices and applications both support the TLS version. Also, make sure that they are enabled for TLS that you want to configure with Unified Communications Manager and IM and Presence Services. If you have any of the following products deployed, confirm that they meet the minimum TLS requirement. If they do not meet this requirement, upgrade those products:

- Skinny Client Control Protocol (SCCP) Conference Bridge
- Transcoder
- Hardware Media Termination Point (MTP)
- SIP Gateway
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment
- Cisco Unified Border Element (CUBE)
- Cisco Expressway
- Cisco TelePresence Conductor

You will not be able to upgrade conference bridges, Media Termination Point (MTP), Xcoder, Prime Collaboration Assurance, and Prime Collaboration Provisioning.

Note If you are upgrading from an earlier release of Unified Communications Manager, make sure that all your devices and applications support the higher version of TLS before you configure it. For example, Unified Communications Manager and IM and Presence Services, Release 9.x supports TLS 1.0 only.

TLS Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	(Optional) Set Minimum TLS Version, on page 20.	By default, Cisco Unified Communications Manager supports a minimum TLS version of 1.0. If your security needs require a higher version of TLS, reconfigure the system to use TLS 1.1 or 1.2.
Step 2	Set TLS Ciphers, on page 21.	Configure an enterprise parameter for the TLS cipher options that Cisco Unified Communications Manager supports.
Step 3	Configure TLS in a SIP Trunk Security Profile, on page 21 .	Assign TLS connections to a SIP Trunk. Trunks that use this profile use TLS for signaling. You can also use the secure trunk to add TLS connections to devices, such as conference bridges.
Step 4	Add Secure Profile to a SIP Trunk, on page 22.	Assign a TLS-enabled SIP trunk security profile to a SIP trunk to allow the trunk to support TLS. You can use the secure trunk to connect resources, such as conference bridges.
Step 5	Configure TLS in a Phone Security Profile, on page 23.	Assign TLS connections to a phone security profile. Phones that use this profile use TLS for signaling.
Step 6	Add Secure Phone Profile to a Phone, on page 23.	Assign the TLS-enabled profile that you created to a phone.
Step 7	(Optional) Add Secure Phone Profile to a Universal Device Template, on page 24.	Assign a TLS-enabled phone security profile to a universal device template. If you have the LDAP directory synchronization configured with this template, you can provision phones with security through the LDAP sync.

Set Minimum TLS Version

By default, Cisco Unified Communications Manager supports a minimum TLS version of 1.0. Use this procedure to reset the minimum supported TLS version for Cisco Unified Communications Manager and the IM and Presence Service to a higher version, such as 1.1 or 1.2.

Before you begin

Make sure that the devices and applications in your network support the TLS version that you want to configure. For details, see TLS Prerequisites, on page 19.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 To confirm the existing TLS version, run the **show tls min-version** CLI command.

Step 3 Run the **set tls min-version** <*minimum*> CLI command where <*minimum*> represents the TLS version.

For example, run **set tls min-version 1.2** to set the minimum TLS version to 1.2.

Step 4 Perform Step 3 on all Cisco Unified Communications Manager and IM and Presence Service cluster nodes.

What to do next

Set TLS Ciphers, on page 21

Set TLS Ciphers

Use this procedure to configure the ciphers that Cisco Unified Communications Manager supports for establishing TLS connections.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 In **Security Parameters**, configure a value for the **TLS Ciphers** enterprise parameter. For help on the available options, refer to the enterprise parameter help.

Step 3 Click **Save**.

What to do next

Configure TLS in a SIP Trunk Security Profile, on page 21

Configure TLS in a SIP Trunk Security Profile

Use this procedure to assign TLS connections to a SIP Trunk Security Profile. Trunks that use this profile use TLS for signaling.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **SIP Trunk Security Profile**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new SIP trunk security profile.

- Click **Find** to search and select an existing profile.

Step 3 In the **Name** field, enter a name for the profile.

Step 4 Configure the **Device Security Mode** field value to **Encrypted** or **Authenticated**.

Step 5 Configure both the **Incoming Transport Type** and **Outgoing Transport Type** field values to **TLS**.

Step 6 Complete the remaining fields of the **SIP Trunk Security Profile** window. For help on the fields and their configuration, see the online help.

Step 7 Click **Save**.

What to do next

Add Secure Profile to a SIP Trunk, on page 22

Add Secure Profile to a SIP Trunk

Use this procedure to assign a TLS-enabled SIP trunk security profile to a SIP trunk. You can use this trunk to create a secure connection to resources, such as conference bridges.

Before you begin

Configure TLS in a SIP Trunk Security Profile, on page 21

Procedure

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

Step 2 Perform one of the following steps:

- Click **Add New** to create a new trunk.
- Click **Find** to search and select an existing trunk.

Step 3 If you are creating a new trunk, select the trunk type and protocol, and click **Next**.

Step 4 For the **Device Name** field, enter a device name for the trunk.

Step 5 From the **Device Pool** drop-down list, choose a device pool.

Step 6 From the **SIP Profile** drop-down list, choose a SIP Profile.

Step 7 From the **SIP Trunk Security Profile** drop-down list, choose the TLS-enabled SIP Trunk Profile that you created in the previous task.

Step 8 In the **Destination** area, enter the destination IP address. You can enter up to 16 destination addresses. To enter additional destinations, click the (+) button.

Step 9 Complete the remaining fields in the **Trunk Configuration** window. For help with the fields and their configuration, see the online help.

Step 10 Click **Save**.

Note If you are connecting the trunk to a secure device, you must upload a certificate for the secure device to Cisco Unified Communications Manager. For certificate details, see the “Certificates” topic of *Security Guide for Cisco Unified Communications Manager*.

What to do next

Configure TLS in a Phone Security Profile, on page 23.

Configure TLS in a Phone Security Profile

Use this procedure to assign TLS connections to a Phone Security Profile. Phones that use this profile use TLS for signaling.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new profile.
- Click **Find** to search and select an existing profile.

Step 3 If you are creating a new profile, select a phone model and protocol, and click **Next**.

Note If you want to use a universal device template and LDAP sync to provision security through the LDAP sync, select **Universal Device Template** as the **Phone Security Profile Type**.

Step 4 Enter a name for the profile.

Step 5 From the **Device Security Mode** drop-down list, select either **Encrypted** or **Authenticated**.

Step 6 (For SIP phones only) From the Transport Type, select **TLS**.

Step 7 Complete the remaining fields of the **Phone Security Profile Configuration** window. For help with the fields and their configuration, see the online help.

Step 8 Click **Save**.

Add Secure Phone Profile to a Phone

Use this procedure to assign the TLS-enabled phone security profile to a phone.

Note To assign a secure profile to a large number of phones at once, use the Bulk Administration Tool to reassign the security profile for them.

Procedure

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

Step 2 Perform one of the following steps:

- Click **Add New** to create a new phone.
- Click **Find** to search and select an existing phone.

Step 3 Select the phone type and protocol and click **Next**.

Step 4 From the **Device Security Profile** drop-down list, assign the secure profile that you created to the phone.

Step 5 Assign values for the following mandatory fields:

- MAC address
- Device Pool
- SIP Profile
- Owner User ID
- Phone Button Template

Step 6 Complete the remaining fields of the **Phone Configuration** window. For help with the fields and their configuration, see the online help.

Step 7 Click **Save**.

Add Secure Phone Profile to a Universal Device Template

Use this procedure to assign a TLS-enabled phone security profile to a universal device template. If you have LDAP directory sync configured, you can include this universal device template in the LDAP sync through a feature group template and user profile. When the sync occurs, the secure profile is provisioned to the phones.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Universal Device Template**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new template.
- Click **Find** to search and select an existing template.

Step 3 For the **Name** field, enter a name for the template.

Step 4 From the **Device Pool** drop-down list, select a device pool.

Step 5 From the **Device Security Profile** drop-down list, select the TLS-enabled security profile that you created.

Note The Phone Security Profile must have been created with **Universal Device Template** as the device type.

Step 6 Select a **SIP Profile**.

Step 7 Select a **Phone Button Template**.

Step 8 Complete the remaining fields of the **Universal Device Template Configuration** window. For help with the fields and their configuration, see the online help.

Step 9 Click **Save**.
Include the Universal Device template in an LDAP directory synchronization. For details on how to set up an LDAP Directory sync, see the "Configure End Users" part of the System Configuration Guide for Cisco Unified Communications Manager.

TLS Interactions and Restrictions

This chapter provides information about the TLS Interactions and Restrictions.

TLS Interactions

Table 5: TLS Interactions

Feature	Interaction
Common Criteria mode	You can enable Common Criteria mode along with configuration of minimum TLS version. If you do so, the applications continue to comply with Common Criteria requirements and disable TLS 1.0 secure connections at application level. When the common criteria mode is enabled, you can configure the minimum TLS version as either 1.1 or 1.2 for the applications. For details on Common Criteria mode, see the Compliance to Common Criteria topic of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

TLS Restrictions

The following table highlights issues that you may run into when implementing Transport Layer Security (TLS) version 1.2 on legacy phones, such as 79xx, 69xx, 89xx, 99xx, 39xx, and IP Communicator. To verify whether your phone supports secure mode in this release, see the Phone Feature List Report in Cisco Unified Reporting. The feature restrictions on legacy phones and the workaround to implement the feature is listed in the following table:

Note The workarounds are designed to get the impacted feature functioning in your system. However, they do not guarantee TLS 1.2 compliance for that feature.

Table 6: Transport Layer Security Version 1.2 Restrictions

Feature	Restriction
Legacy phones in Encrypted Mode	Legacy phones in Encrypted Mode do not work. There is no workaround.
Legacy phones in Authenticated Mode	Legacy phones in Authenticated Mode do not work. There is no workaround.
IP Phone services using secure URLs based on HTTPS.	IP Phone services using secure URLs based on HTTPS do not work. Workaround to use IP Phone services: Use HTTP for all underlying service options. For example, corporate directory and personal directory. However, HTTP is not recommended as HTTP is not as secure if you need to enter sensitive data for features, such as Extension Mobility. The drawbacks of using HTTP include: • Provisioning challenges when configuring HTTP for legacy phones and HTTPS for supported phones. • No resiliency for IP Phone services. • Performance of the server handling IP phone services can be affected.

Feature	Restriction
Extension Mobility Cross Cluster (EMCC) on legacy phones	EMCC is not supported with TLS 1.2 on legacy phones. Workaround: Complete the following tasks to enable EMCC: **1.** Enable EMCC over HTTP instead of HTTPS. **2.** Turn on mixed-mode on all Unified Communications Manager clusters. **3.** Use the same USB eTokens for all Unified Communications Manager clusters.
Locally Significant Certificates (LSC) on legacy phones	LSC is not supported with TLS 1.2 on legacy phones. As a result, 802.1x and phone VPN authentication based on LSC are not available. Workaround for 802.1x: Authentication based on MIC or password with EAP-MD5 on older phones. However, those are not recommended. Workaround for VPN: Use phone VPN authentication based on end-user username and password.
Encrypted Trivial File Transfer Protocol (TFTP) configuration files	Encrypted Trivial File Transfer Protocol (TFTP) configuration files are not supported with TLS 1.2 on legacy phones even with Manufacturer Installed Certificate (MIC). There is no workaround.
CallManager certificate renewal causes legacy phones to lose trust	Legacy phones lose trust when CallManager certificate is renewed. For example, a phone cannot get new configurations after renewing the certificate. This is applicable only in Unified Communications Manager 11.5.1 Workaround: To prevent legacy phones from losing trust, complete the following steps: **1.** Before you enable the CallManager certificate, set the **Cluster For Roll Back to Pre 8.0** enterprise parameter to **True**. By default, this setting disables the security. **2.** Temporarily allow TLS 1.0 (multiple Unified Communications Manager reboots).
Connections to non-supported versions of Cisco Unified Communications Manager	TLS 1.2 connections to older versions of Unified Communications Manager that do not support the higher TLS version do not work. For example, a TLS 1.2 SIP trunk connection to Unified Communications Manager Release 9.x does not work because that release does not support TLS 1.2. You can use one of the following workarounds: • Workaround to enable connections: Use nonsecure trunks, although this is not a recommended option. • Workaround to enable connections while using TLS 1.2: Upgrade the non-supported version to a release that does support TLS 1.2.

Feature	Restriction
Certificate Trust List (CTL) Client	CTL client does not support TLS 1.2. You can use one of the following workarounds: • Temporarily allow TLS 1.0 when using the CTL client and then move the Cluster to Common Criteria mode. Configure Minimum TLS to 1.1 or 1.2 • Migrate to the Tokenless CTL by using the CLI Command **utils ctl set-cluster mixed-mode** in Common Criteria mode. Configure Minimum TLS to 1.1 or 1.2
Address Book Synchronizer	There is no workaround.

Cisco Unified Communications Manager Ports Affected by Transport Layer Security Version 1.2

The following table lists the Unified Communications Manager Ports Affected By TLS Version 1.2

Table 7: Cisco Unified Communications Manager Ports Affected by Transport Layer Security Version 1.2

Application	Protocol	Destination / Listener	Cisco Unified Communications Manager Operating in Normal mode			Cisco Unified Communications Manager Operating in Common Criteria Mode		
			Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2
Tomcat	HTTPS	443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS v1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
SCCP - SEC - SIG	Signalling Connection Control Part (SCCP)	2443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
CTL-SERV	Proprietary	2444	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
Computer Telephony Integration (CTI)	Quick Buffer Encoding (QBE)	2749	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
CAPF-SERV	Transmission Control Protocol (TCP)	3804	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2

Application	Protocol	Destination / Listener	Cisco Unified Communications Manager Operating in Normal mode			Cisco Unified Communications Manager Operating in Common Criteria Mode		
			Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2
Intercluster Lookup Service (ILS)	Not applicable	7501	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
Administrative XML (AXL)	Simple Object Access Protocol (SOAP)	8443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
High Available-Proxy (HA-Proxy)	TCP	9443	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.2	TLS 1.2
SIP-SIG	Session Initiation Protocol (SIP)	5061 (configurable with trunk)	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
HA Proxy	TCP	6971, 6972	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
Cisco Tomcat	HTTPS	8080, 8443	8443: TLS 1.0, TLS 1.1, TLS 1.2	8443: TLS 1.1, TLS 1.2	8443: TLS 1.2	TLS 1.1	8443: TLS 1.1, TLS 1.2	8443: TLS 1.2
Trust Verification Service (TVS)	Proprietary	2445	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2

Instant Messaging and Presence Ports Affected by Transport Layer Security Version 1.2

The following table lists the IM and Presence Service Ports Affected By Transport Layer Security Version 1.2:

Table 8: Instant Messaging & Presence Ports Affected by Transport Layer Security Version 1.2

Destination/Listener	Instant Messaging & Presence Operating in Normal mode			Instant Messaging & Presence Operating in Common Criteria mode		
	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2
443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
5061	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
5062	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
7335	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
8083	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
8443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2

Push Notifications Enhancements for Cisco Jabber on iPhone and iPad

With this release, the Push Notifications for Cisco Jabber on iPhone and iPad solution has been enhanced with the following updates:

- Voice and Video Call Support—Cisco Unified Communications Manager now uses Push Notifications to send voice and video calls to Cisco Jabber on iPhone or iPad clients that are in suspended mode. This update removes the need to use the cellular network to reach Jabber on iPhone and iPad clients that are in suspended mode, thereby decreasing your network costs.
- High Availability for IM and Presence—This release adds failover protection for Push Notifications-enabled IM and Presence sessions over Cisco Jabber on iPhone or iPad. With this feature, the backup node in the subcluster can take over a failed session without a need for any user action. The backup node can completely recreate the IM session so that the user does not lose the IM history.
- Troubleshooting Options—This release provides additional troubleshooting options for troubleshooting and debugging your system. This ensures that your system remains up and running at all times.

For additional detail on the Push Notifications solution with Release 11.5(1)SU3, refer to *Deploying Push Notifications for Cisco Jabber on iPhone and iPad* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/pushNotifications/11_5_1_su2/cucm_b_push-notification-deployment-iPhone-iPad.html.

User Interface Updates

With this release, the **Enable Push Notifications and Send Troubleshooting and Analytics Information to Cisco Cloud** check box in the **Cisco Cloud Onboarding** window has been replaced with the following new fields:

- **Enable Push Notifications**— Check this check box to enable Push Notifications voice, video and IM and Presence support for Cisco Jabber on iPhone and iPad clients.
- **Send Troubleshooting information to the Cisco cloud**—When the check box is checked, Cisco Unified Communications Manager and IM and Presence Service cluster sends alarm syslog files at regular intervals to the Cisco Cloud. Cisco uses this information for proactive debugging and problem resolution.
- **Send encrypted PII to the Cisco cloud for troubleshooting**—When this check box is checked, Cisco Unified Communications Manager encrypts all troubleshooting data that can be used to identify the partner before sending to the Cisco Cloud (for example, device names or hostnames).

CLI Commands for Troubleshooting Push Notifications

Push Notifications provides the following CLI commands, which can be run on the Unified Communications Manager publisher node for troubleshooting:

- **utils managementAgent alarms pushfrequency**—Run this command to configure the interval following which Cisco Unified Communications Manager sends Push Notifications alarms to the Cisco Cloud. The default value is 30 minutes.
- **utils managementAgent alarms pushlevel**—Run this command to configure the minimum severity level for which Cisco Unified Communications Manager sends Push Notifications alarms to the Cisco Cloud. The default severity is `Error`.
- **utils managementAgent alarms pushnow**—Run this command to upload Push Notifications alarms to the Cisco Cloud immediately, without waiting for the interval to expire.

TLS as a Communication Protocol for Syslog and FileBeat

Cisco Unified Communications Manager and IM and Presence Service will be made Common Criteria compliant from version 11.5.1 SU3 onwards. It is mandatory to use Transport Layer Security (TLS) 1.2 as a communication protocol to comply with Common Criteria guidelines. As of Release 11.5(1) SU2, Transport Layer Security (TLS) 1.2 can be used as a communication protocol for syslog and FileBeat. 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.
- In Common Criteria Mode, strict host name verification will be implemented. Hence, it is required to configure the server with a fully qualified domain name (FQDN) which matches the certificate.

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.

Upgrade External Database Table Values for Microsoft SQL Datatype

In earlier versions of IM and Presence Service, there was no option to write Unicode characters to a persistent chat room when Microsoft SQL server is configured as external database.

With this release, Microsoft SQL Datatype values are upgraded from text to nvarchar (new size) and varchar (existing size) to nvarchar (existing size) in the following tables:

- AFT_LOG Table
- TC_ROOMS Table
- TC_USERS Table
- TC_MESSAGES Table
- TC_TIMELOG Table
- TC_MSGARCHIVE Table

- JM Table

For detailed information on Microsoft SQL Datatype values, refer to *Database Setup for IM and Presence Service on Cisco Unified Communications Manager, Release 11.5(SU3)*.