New and Changed Features

- JTAPI Plugin Support, on page 2
- Oracle JRE Removal from Manager Assistant, on page 2
- Branding Customizations, on page 2
- Centralized Deployment for IM and Presence, on page 4
- Cisco Jabber Authentication via OAuth Refresh Logins, on page 8
- Compliance Enhancement for IM and Presence, on page 11
- Compliance to Common Criteria, on page 11
- Configure SIP Trunk to Distinguish Between Trusted and Untrusted Caller Identities, on page 18
- Configure Exchange 2016 as a Presence Gateway over Exchange Web Services, on page 19
- Deprecated Phone Models, on page 20
- Emergency Notifications Paging, on page 22
- Enhanced CTL and ITL Phone Trust and Migration, on page 22
- Enhanced Usability in the User Device Association Screen, on page 25
- External Database Cleanup Utility for IM and Presence, on page 25
- External Database Text Conferencing Report, on page 26
- Extension Mobility Roaming Across Clusters, on page 26
- Home Cluster Routing Through Session Management Edition for Cisco Spark Hybrid Call Service Connect, on page 27
- IPv6-only Network, on page 28
- Independent Audio and Video Bit Rates for Video Calls, on page 31
- Minimum TLS Version Control, on page 32
- Mobile and Remote Access Policy for Jabber, on page 35
- New Certificate Added to the Trust Store, on page 36
- New Columns to Manage Devices Efficiently, on page 37
- New Sign-In Options for Extension Mobility Users, on page 39
- Non-compliance to FIPS, on page 39
- IPsec Requirements, on page 40
- SAML SSO Support for Cisco Unified Communications Manager Web Interfaces, on page 40
- SAML SSO Okta Identity Provider, on page 44
- Smart Software Licensing , on page 44
- Supported LDAP Directories , on page 53
- Voicemail Launch from Self Care Portal, on page 53
- Web Browser Security Enhancement, on page 54

• Web Browser Support, on page 54

JTAPI Plugin Support

Starting from Release 12.0(1)SU4 and all subsequent SU or ES releases in this release train, the Cisco JTAPI 32-bit plugin support is EOL for download from the Cisco Unified CM Administration interface.

Also, the bundled Oracle JRE is removed for the 64-bit JTAPI plugin and therefore requires JRE to be installed on the system for the plugin to work before the user upgrades to the newer version.

For more information, refer sections "Installing Cisco JTAPI on 64 bit Windows Platforms" at Cisco Unified JTAPI Developers Guide for Cisco Unified Communications Manager 12.0(1).

Oracle JRE Removal from Manager Assistant

The Oracle Java Runtime Environment (JRE) is no longer included in the Cisco Unified Communications Manager Assistant plug-in.

Before you upgrade the Cisco Unified Communications Manager Assistant client to a newer version, perform the following:

- Uninstall the Cisco Unified Communications Manager Assistant client that is currently installed on your machine.
- Install JRE on 32-bit or 64-bit Windows platform.

For more information, see the Feature Configuration Guide for Cisco Unified Communications Manager.

Branding Customizations

The Branding feature lets you upload customized branding for Cisco Unified Communications Manager and IM and Presence Service. Branding gets applied to the Cisco Unified CM Administration or Cisco Unified CM IM and Presence Administration login and configuration windows. Among the items that you can modify include:

- Company logos
- Background colors
- Border colors
- Font colors

Branding Configuration

Branding must be enabled separately for the Cisco Unified Communications Manager and IM and Presence Service user interfaces:

- For details on how to enable Branding for the Unified Communications Manager interface, and how to append a company logo to the Self-Care Portal interface, see the "Branding Customizations" chapter of the Feature Configuration Guide for Cisco Unified Communications Manager, Release 12.0(1).

- For details on how to enable Branding for the IM and Presence Service interface, see the "Branding Customizations" chapter of the Configuration and Administration Guide for the IM and Presence Service, Release 12.0(1).

Append Logo in Self Care Portal

The Branding feature allows you to append your company logo to the Unified Communications Self Care Portal login page and to the user interface header. You must include the `branding_logo.png` file in your `branding.zip` file and upload the zip file into Unified Communications Manager. The logo displays in the Self Care Portal after you enable branding in Unified Communications Manager.

There is no option to customize background colors or fonts for the Self-Care portal.

New CLI Commands

The following CLI commands have been introduced to support the Branding feature. You must have Command privilege level 4 access to run these commands:

- **utils branding enable**—Run this command to enable branding on a node.
- **utils branding disable**—Run this command to disable branding on a node.
- **utils branding status**—Run this command to see the status of whether branding is enabled or disabled on a node.

Online Help Updates

The following table displays the online help updates for the Branding feature. The fields are the same for both Cisco Unified Communications Manager and IM and Presence Service. However, the Self-Care Portal is updated automatically only when you enable branding in Unified Communications Manager.

The Branding menu can be accessed from Cisco Unified OS Administration or Cisco Unified CM IM and Presence OS Administration interface by selecting **Software Upgrades** > **Branding**.

Table 1: Branding Field Settings

Field	Description
Browse	Click this button to search for and select your `branding.zip` file
Upload File	Click this button to upload the `branding.zip` file to your system. For more information on creating `branding.zip` file according to the prescribed specifications and applying this customized branding to your system, see topic related to branding file requirements in the *Feature Configuration Guide for Cisco Unified Communications Manager*.
Enable Branding	After you have uploaded the `branding.zip` file, click this button to enable branding customizations on this Unified Communications Manager node. After you enable branding, refresh your browser. **Note** Enabling branding also appends your company logo to the Unified Communications Self Care Portal.

Field	Description
Disable Branding	Click this button to disable customized branding from Unified Communications Manager. **Note** Disabling branding also removes the company logo from the Unified Communications Self-Care Portal.

Centralized Deployment for IM and Presence

The IM and Presence centralized deployment allows you to deploy your IM and Presence deployment and your telephony deployment in separate clusters. The central IM and Presence cluster handles IM and Presence for the enterprise, while the remote Cisco Unified Communications Manager telephony cluster handles voice and video calls for the enterprise.

The Centralized Deployment option provides the following benefits when compared to standard deployments:

- The Centralized Deployment option does not require a 1x1 ratio of telephony clusters to IM and Presence Service clusters–you can scale your IM and Presence deployment and your telephony deployment separately, to the unique needs of each.
- Full mesh topology is not required for the IM and Presence Service
- Version independent from telephony–your IM and Presence central cluster can be running a different version than your Cisco Unified Communications Manager telephony clusters.
- Can manage IM and Presence upgrades and settings from the central cluster.
- Lower cost option, particularly for large deployments with many Cisco Unified Communications Manager clusters
- Easy XMPP Federation with third parties.
- Supports calendar integration with Microsoft Outlook. For configuration details, refer to the document *Microsoft Outlook Calendar Integration for the IM and Presence Service*.

Centralized Deployment Setup vs Standard (Decentralized) Deployments

The following table discusses some of the differences in setting up an IM and Presence Centralized Cluster Deployment as opposed to standard deployments of the IM and Presence Service.

Setup Phase	Differences with Standard Deployments
Installation Phase	The installation process for an IM and Presence central deployment is the same as for the standard deployment. However, with central deployments, the IM and Presence central cluster is installed separately from your telephony cluster, and may be located on separate hardware servers. Depending on how you plan your topology, the IM and Presence central cluster may be installed on separate physical hardware from your telephony cluster. For the IM and Presence central cluster, you must still install Cisco Unified Communications Manager and then install the IM and Presence Service on the same servers. However, the Cisco Unified Communications Manager instance of the IM and Presence central cluster is for database and user provisioning primarily, and does not handle voice or video calls.
Configuration Phase	Compared to standard (decentralized) deployments, the following extra configurations are required to set up the IM and Presence Service Central Deployment: • Users must be synced into both the telephony cluster and the IM and Presence Service central cluster so that they exist in both databases. • In your telephony clusters, end users should not be enabled for IM and Presence. • In your telephony clusters, the Service Profile must include the IM and Presence Service and must point to the IM and Presence central cluster. • In the IM and Presence central cluster, users must be enabled for the IM and Presence Service. • In the IM and Presence central cluster's database publisher node, add your remote Cisco Unified Communications Manager telephony cluster peers. The following configurations, which are used with Standard Deployments of the IM and Presence Service, but are not required with Central Deployments: • A Presence Gateway is not required. • A SIP Publish trunk is not required. • A Service Profile is not required on the IM and Presence central cluster—the Service Profile is configured on the telephony cluster to which the central cluster connects.

The IM and Presence centralized deployment allows you to deploy your IM and Presence deployment and your telephony deployment in separate clusters. The central IM and Presence cluster handles IM and Presence for the enterprise, while the remote Cisco Unified Communications Manager telephony cluster handles voice and video calls for the enterprise.

The Centralized Deployment option provides the following benefits when compared to standard deployments:

- The Centralized Deployment option does not require a 1x1 ratio of telephony clusters to IM and Presence Service clusters–you can scale your IM and Presence deployment and your telephony deployment separately, to the unique needs of each.

- Full mesh topology is not required for the IM and Presence Service
- Version independent from telephony–your IM and Presence central cluster can be running a different version than your Cisco Unified Communications Manager telephony clusters.
- Can manage IM and Presence upgrades and settings from the central cluster.
- Lower cost option, particularly for large deployments with many Cisco Unified Communications Manager clusters
- Easy XMPP Federation with third parties.
- Supports calendar integration with Microsoft Outlook. For configuration details, refer to the document *Microsoft Outlook Calendar Integration for the IM and Presence Service*.

Interclustering for Centralized Deployment

Interclustering is supported between two centralized clusters. Intercluster peering is tested with one cluster with 25K (with 25K OVA) and another with 15K (with 15K OVA) devices and no performance issues were observed.

User Interface Updates

To manage this feature, the **Centralized Deployment** window has been added to the **System** menu of the Cisco Unified Communications Manager IM and Presence Administration interface. Administrators can add their remote Cisco Unified Communications Manager clusters to the IM and Presence central cluster in this window.

Configuration

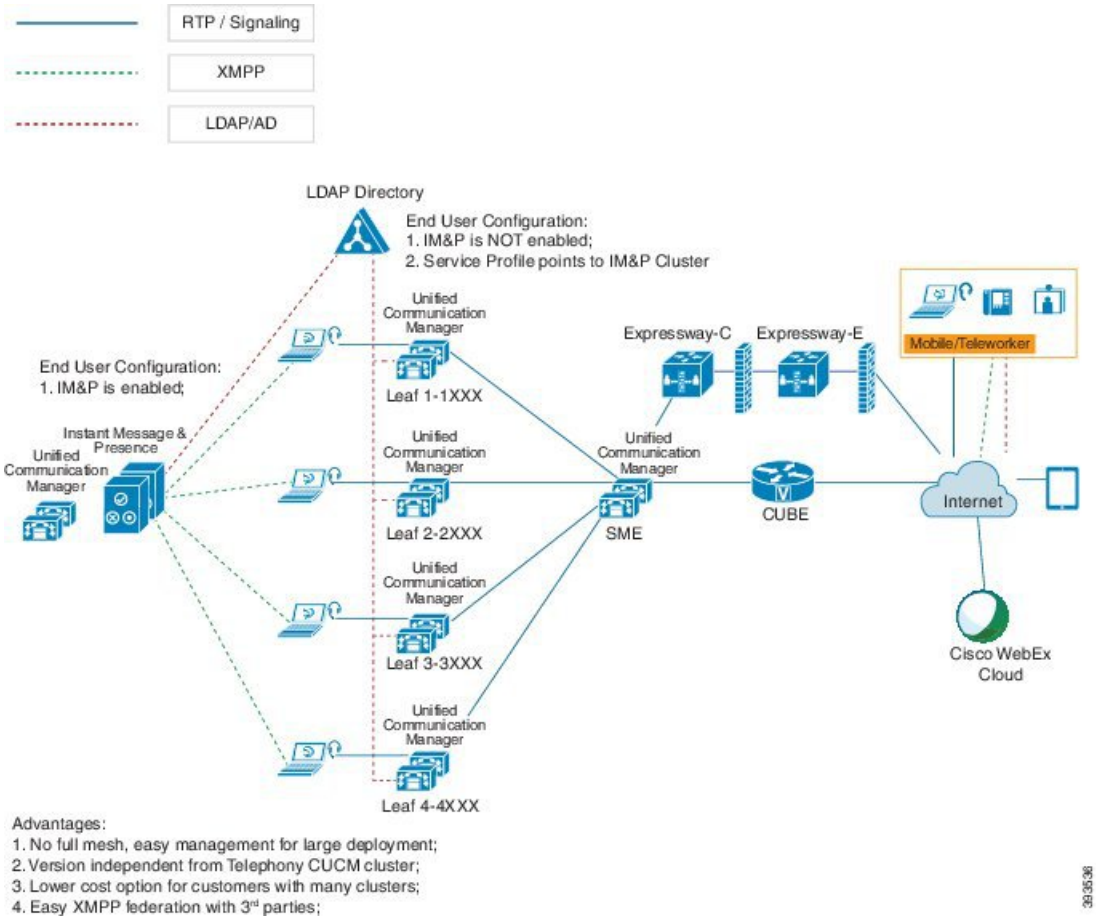
For detailed procedures on how to configure an IM and Presence Service centralized deployment, see the "Configure Centralized Deployment" chapter of the Configuration and Administration Guide for the IM and Presence Service.

Centralized Cluster Deployment Architecture

The following diagram highlights the cluster architecture for this deployment option. Cisco Jabber clients connect to multiple Cisco Unified Communications Manager clusters for voice and video calling. In this example, the Cisco Unified Communications Manager telephony clusters are leaf clusters in a Session Management Edition deployment. For Rich Presence, Cisco Jabber clients connect to the IM and Presence Service central cluster. The IM and Presence central cluster manages instant messaging and presence for the Jabber clients.

Note Your IM and Presence cluster still contains an instance for Cisco Unified Communications Manager. However, this instance is for handling shared features such as database and user provisioning–it does not handle telephony.

Figure 1: IM and Presence Service Centralized Cluster Architecture

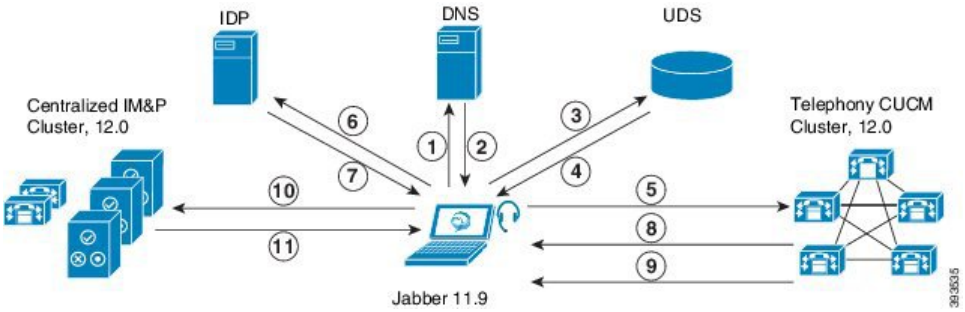


Centralized Cluster Use Case

To connect your telephony and IM and Presence clusters, a new system for exchanging access keys is introduced. This diagram shows the flow for SSO logins:

- [1]-[2]: Query DNS to get SRV record.
- [3]-[4]: Query UDS to get the Home Cisco Unified Communications Manager cluster.
- [5]-[8]: Get Access Token and Refresh Token from Cisco Unified Communications Manager cluster through SAML SSO.
- [9]: Read UC Service Profile. The service profile contains an IM and Presence profile and points to the IM and Presence central cluster.
- [10]: Client registers to the IM and Presence cluster using the same Access Token through SOAP and XMPP interfaces.
- [11]: The token is validated and a response is sent back to Jabber client.

Figure 2: IM and Presence Service Centralized Cluster Use Case



Centralized Deployment Field Descriptions

From Cisco Unified CM IM and Presence Administration, choose **System** > **Centralized Deployment** to access the Centralized Deployment window. If you are deploying the IM and Presence Centralized Cluster deployment, you can create connections to your remote Cisco Unified Communications Manager clusters in this configuration window.

Click the **Add New** button to add a Cisco Unified Communications Manager cluster. Click **Synchronize Selected** to synchronize access keys with the remote cluster.

Table 2: Centralized Deployment Field Descriptions

Field	Description
Peer Address	The FQDN, hostname, IPv4 address, or IPv6 address of the remote Cisco Unified Communications Manager cluster publisher node. **Note** The Peer Address cannot point to any IM and Presence Service node or to the Cisco Unified Communications Manager instance of another IM and Presence Service central cluster.
Peer AXL Username	The login username for the AXL account on the remote cluster.
Peer AXL Password	The password for the AXL account on the remote cluster.
Status	Displays the current sync status with the remote cluster.
Last Synchronized	Displays the last time a sync occurred with the remote cluster.
Save and Synchronize	After you have entered your details, click this button to save your settings and to sync access keys with the remote cluster.

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.

Configuration Details

To configure OAuth Refresh Logins, see the "Configure Cisco Jabber" of the System Configuration Guide for Cisco Unified Communications Manager, Release 12.0(1).

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 3: 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`

Compliance Enhancement for IM and Presence

The Message Archiver feature for IM and Presence Service has been updated to include an option that mandates that all messages are archived, in case of a compliance database outage. This update helps companies in regulated industries comply with guidelines that require business record archiving.

In previous releases, if the Message Archiver was configured, but the connection to the external Compliance database went down, instant messaging could continue without being archived. With this release, the Message Archiver feature includes an option where all messaging stops while the external compliance database is down. Messaging continues only after the compliance database comes up again thus ensuring that all instant messaging is archived.

For more information about how to configure the Message Archiver, see the Instant Messaging Compliance Guide for IM and Presence Service.

User Interface Updates for Message Archiver

To support this feature, a new check box is added to the Compliance Settings window. This check box appears if you select the **Message Archiver** option:

Block message delivery if unable to record in compliance database

- Check—If messages are not archived then instant messaging stops and Jabber users get notification that “Message to user could not be delivered."
- Uncheck—If messages are not archived then messaging continues with no interruption and Jabber users have no way of knowing that messages are not archived.

Compliance to Common Criteria

With Release 12.0(1), 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.

CLI Reference Guide Updates

The following CLI commands are included in the *CLI Reference Guide for Cisco Unified Communications Solutions* to support Common Criteria.

utils fips_common_criteria

This command configures the Common Criteria mode in the system.

utils fips_common_criteria {**enable** | **disable** | **status**}

Syntax Description

Parameters	Description
enable	Enables the Common Criteria mode in the system
disable	Disables the Common Criteria mode in the system When Common Criteria mode is disabled, a prompt is displayed to set the minimum TLS version.
status	Displays the status of Common Criteria mode in the system

Command Modes

Administrator (admin:)

Usage Guidelines

Secure connections using TLS version 1.0 are not permitted after enabling the Common Criteria mode. FIPS mode will be enabled while enabling Common Criteria mode. Enabling or disabling Common Criteria mode does not require certificates to be regenerated. However, enabling or disabling FIPS does require rebooting of the system along with regeneration of certificates.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and IM and Presence Service

Note This CLI command is not applicable to Cisco Unity Connection.

utils fips

Caution FIPS mode is only supported on releases that have been through FIPS compliance. Be warned that FIPS mode should be disabled before you upgrade to a non-FIPS compliance version of Unified Communications Manager.

For information about which releases are FIPS compliant and to view their certifications, see the *FIPS 140* document at https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html.

This command enables, disables, or displays the status of FIPS 140-2 mode. FIPS 140-2 mode is disabled by default; only an administrator can enable FIPS.

utils fips {**enable** | **disable** | **status**}

Syntax Description

Parameters	Description
enable	Activates FIPS 140-2 mode.
disable	Deactivates FIPS 140-2 mode.
status	Displays the status of FIPS 140-2 mode.

Command Modes

Administrator (admin:)

Usage Guidelines

Before enabling FIPS mode, we recommend that you perform a system backup. If FIPS checks fail at start-up, the system halts and requires a recovery CD to be restored.

Consider the following information before you enable FIPS 140-2 mode:

- When you switch from non-FIPS to FIPS mode, the MD5 and DES protocols will not be functional.
- After FIPS mode is enabled on a server, please wait until the server reboots and the phones re-register successfully before enabling FIPS on the next server.
- In FIPS mode, the IM and Presence service uses Red Hat Openswan (FIPS validated) in place of Racoon (non-FIPS validated). If the security policies in Racoon contain functions that are not FIPS approved, the CLI command asks you to redefine the security policies with FIPS approved functions and abort.

Note Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.

Consider the following information before you disable FIPS 140-2 mode: In multiple server clusters, each server must be disabled separately; FIPS mode is not disabled cluster-wide but on a per server basis.

Consider the following information after you enable FIPS 140-2 mode: If you have a single server cluster and chose to apply "Prepare Cluster for Rolback to pre 8.0" enterprise parameter before enabling FIPS mode, disable this parameter after making sure that all the phones registered successfully with the server.

Consider the following information before you enable or disable FIPS 140-2 mode for IM and Presence Service: After you enable or disable FIPS 140-2 mode for IM and Presence Service, the Tomcat certificate is regenerated and the node reboots. The Intercluster Sync Agent syncs the new Tomcat certificate across the

cluster; this can take up to 30 minutes. Until the new Tomcat certificate is synced across the cluster, an IM and Presence Servicee subscriber node cannot access information from the IM and Presence Service database publisher node. For example, a user who is logged into the Cisco Unified Serviceability GUI on a subscriber node will not be able to view services on theIM and Presence Service database publisher node. Users will see the following error message until the sync is complete: `Connection to server cannot be established (certificate exception)`

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection

Security Guide Updates

These topics are added to the *FIPS 140-2 Setup* chapter of the *Security Guide for Cisco Unified Communications Manager, Release 12.0(1)*. These topics include configuring TLS for common criteria mode, prerequisites, and configuring common criteria mode.

Common Criteria Configuration Task Flow

- FIPS mode must be running to enable Common Criteria mode. If FIPS isn't already enabled, you'll be prompted to enable it when you try to enable Common Criteria mode. Enabling FIPS does require certificate regeneration. For more information, see Enable FIPS 140-2 Mode, on page 14.
- X.509 v3 certificates are required in Common Criteria mode. X.509 v3 certificates enable secure connections when using TLS 1.2 as a communication protocol for the following:
  - Remote audit logging
  - Establishing connection between the FileBeat client and the logstash server.

To configure Unified Communications Manager and IM and Presence Service for Common Criteria mode, perform the following:

Procedure

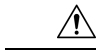
	Command or Action	Purpose
Step 1	Enable TLS, on page 16	TLS is a prerequisite for configuring Common Criteria mode.
Step 2	Configure Common Criteria Mode, on page 17	Configure Common Criteria mode on all Unified Communications Manager and IM and Presence Service cluster nodes.

Enable FIPS 140-2 Mode

Consider the following before you enable FIPS 140-2 mode on Unified Communications Manager:

- When you switch from non-FIPS to FIPS mode, the MD5 and DES protocols aren't functional.

- In single server clusters, because certificates are regenerated, you need to run the CTL Client or apply the Prepare Cluster for Rollback to pre-8.0 enterprise parameter before you enable FIPS mode. If you do not perform either of these steps, you must manually delete the ITL file after you enable FIPS mode.
- After you enable FIPS mode on a server, please wait until the server reboots and the phones re-register successfully before enabling FIPS on the next server.



Caution Before you enable FIPS mode, we strongly recommend that you perform a system backup. If FIPS checks fail at start-up, the system halts and requires a recovery CD to be restored.

Procedure

Step 1 Start a CLI session.

For more information, see "Start CLI Session" in the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Step 2 In the CLI, enter **utils fips enable**

If you enter a password less than 14 characters, the following prompt appear:

```
The cluster security password must be at least 14 characters long before
 security modes such as FIPS, Common Criteria and Enhanced Security modes can be
 enabled. Update the cluster security password using the 'set password user
security' CLI command on all nodes and retry this command.
**************************************************************************
Executed command unsuccessfully
```

If you enter a password more than 14 characters, the following prompts appear:

```
Security Warning: The operation will regenerate certificates for

1)CallManager
2)Tomcat
3)IPsec
4)TVS
5)CAPF
6)SSH
7)ITLRecovery
Any third party CA signed certificates that have been uploaded for the above
components will need to be re-uploaded. If the system is operating in mixed
mode, then the CTL client needs to be run again to update the CTL file.
If there are other servers in the cluster, please wait and do not change
the FIPS Settings on any other node until the FIPS operation on this node
is complete and the system is back up and running.

If the enterprise parameter 'TFTP File Signature Algorithm' is configured
with the value 'SHA-1' which is not FIPS compliant in the current version of the
Unified Communications Manager, though the signing operation
will continue to succeed, it is recommended the parameter value be changed to
SHA-512 in order to be fully FIPS. Configuring SHA-512 as the signing algorithm
may reqiure all the phones that are provisioned in the cluster to be capable of
verifying SHA-512 signed configuration file, otherwise the phone registration
may fail. Please refer to the Cisco Unified Communications Manager Security Guide
```

```
for more details.
********************************************************************************
This will change the system to FIPS mode and will reboot.
********************************************************************************

WARNING: Once you continue do not press Ctrl+C. Canceling this operation after
it
starts will leave the system in an inconsistent state; rebooting the system and
running "utils fips status" will be required to recover.
********************************************************************************
Do you want to continue (yes/no)?
```

Step 3 Enter **Yes**.

The following message appears:

```
Generating certificates...Setting FIPS mode in operating system.
FIPS mode enabled successfully.
******************************************************
It is highly recommended that after your system restarts
that a system backup is performed.
******************************************************
The system will reboot in a few minutes.
```

Unified Communications Manager reboots automatically.

Note
- Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.
- If you have a single server cluster and applied the **Prepare Cluster for Rollback to pre 8.0** enterprise parameter before you enabled FIPS 140-2 mode, you must disable this enterprise parameter after making sure that all the phones registered successfully to the server.

Note In FIPS mode, Unified Communications Manager uses Libreswan (FIPS validated) in place of Racoon (non-FIPS validated). If the security policies in Racoon contain functions that aren't FIPS approved, CLI command asks you to redefine security policies with FIPS approved functions and abort. For more information, see topics related to IPsec Management in the Administration Guide for Cisco Unified Communications Manager.

Enable TLS

TLS 1.2 version or TLS version 1.1 is a requirement for Common Criteria mode. Secure connections using TLS version 1.0 are not permitted after enabling Common Criteria mode.

- During establishment of a TLS connection, the `extendedKeyUsage` extension of the peer certificate is checked for proper values.
  - The peer certificate should have `serverAuth` as `extendedKeyUsage` extension if the peer is a server.
  - The peer certificate should have `clientAuth` as `extendedKeyUsage` extension if the peer is a client.

If the `extendedKeyUsage` extension does not exist in the peer certificate or is not set properly, the connection is closed.

To support TLS version 1.2, perform the following:

Procedure

Step 1 Install Soap UI version 5.2.1.

Step 2 If you are running on the Microsoft Windows platform:

a) Navigate to `C:\Program Files\SmartBear\SoapUI-5.2.1\bin`.

b) Edit the `SoapUI-5.2.1.vmoptions` file to add `-Dsoapui.https.protocols=TLSv1.2,TLSv1,SSLv3` and save the file.

Step 3 If you are running on Linux, edit the `bin/soaup.sh` file to add `JAVA_OPTS="$JAVA_OPTS -Dsoapui.https.protocols=SSLv3,TLSv1.2"` and save the file.

Step 4 If you are running OSX:

a) Navigate to `/Applications/SoapUI-{VERSION}.app/Contents`.

b) Edit the `vmoptions.txt` file to add `-Dsoapui.https.protocols=TLSv1.2,TLSv1,SSLv3` and save the file.

Step 5 Restart the SoapUI tool and proceed with AXL testing

Configure Common Criteria Mode

Use this procedure to configure Common Criteria mode for Unified Communications Manager and IM and Presence Service Service.

Procedure

Step 1 Log in to the Command Line Interface prompt.

Step 2 Run `utils fips_common_criteria status` command to verify whether the system is operating in Common Criteria mode.

Step 3 Run one of the following commands on a cluster node:

- To enable the Common Criteria mode, run `utils fips_common_criteria enable`.
- To disable the Common Criteria mode, run `utils fips_common_criteria disable`.

  When Common Criteria mode is disabled, a prompt is displayed to set the minimum TLS version.

Note Do not run these commands on all nodes simultaneously.

Step 4 To enable Common Criteria Mode across a single cluster, repeat this procedure on all Unified Communications Manager and IM and Presence Service cluster nodes.

Note

- CTL client does not connect to Unified Communications Manager node when server is in the Common Criteria mode, as CTL client does not support TLS 1.1 and TLS 1.2 protocols.
- Only phone models that support TLS 1.1 or TLS 1.2 such as DX series and 88XX series phones are supported in Common Criteria mode. Phone models that support only TLSv1.0 such as 7975 and 9971 are not supported in the Common Criteria mode.
- 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 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.

Step 5 To enable the Common Criteria mode in a multi cluster setup where ICSA is already configured between the nodes, enable Common Criteria mode in each of the nodes in the following order:

a. Unified Communications Manager - Cluster 1 (Publisher)

b. IM and Presence Service - Cluster 1 (Publisher)

c. IM and Presence Service - Cluster 1 (Subscriber or subscribers)

d. Unified Communications Manager - Cluster 2 (Publisher)

e. IM and Presence Service - Cluster 2 (Publisher)

f. IM and Presence Service - Cluster 2 (Subscriber or subscribers)

Step 6 In case of a cert sync failure, see.

Configure SIP Trunk to Distinguish Between Trusted and Untrusted Caller Identities

Call anchoring enables a call to proceed as if it originated from an endpoint registered to CUCM. Anchoring calls without trustworthy caller identity creates a vulnerability to toll and impersonation fraud.

As of Release 12.0.1, SIP trunks can be configured to distinguish between trusted and untrusted caller identities in From header, Remote-party ID (RPID) header, P-Preferred Identity (PPI) header, and P-Asserted Identity (PAI) header. Calls are anchored based on whether the SIP trunk is configured to trust a caller identity.

User Interface Updates

A new dropdown **Trust Received Identity** has been **Trunk Configuration** window in Cisco Unified Communications Manager. Users can set the following options:

- **Trust All (Default)**—Trusts all identities in an incoming message to a SIP trunk. The identities that are trusted include From header, Remote-party ID (RPID) header, P-Preferred Identity (PPI) header, and P-Asserted Identity (PAI) header.

  This is the default value.

- **Trust PAI Only**—Trusts only P-Asserted Identity in an incoming message to a SIP trunk. The identities that are not trusted include From, RPID, and PPI.
- **Trust None**—Never trusts the identities in an incoming message to a SIP trunk. The identities that are not trusted include From, RPID, PPI and PAI.

Note This setting affects the Cisco Unified Mobility Call anchoring feature. The specified value affects the call anchoring feature in the following ways:

- **Trust All (Default)**—Calls are anchored if the identity in From, RPID, PPI, or PAI header matches a Directory Number (DN) or Directory URI (DURI) of a configured remote destination on the Unified Communications Manager.
- **Trust PAI Only**—Calls are anchored only if the identity in the PAI header matches a DN or DURI of a configured remote destinations on the Unified Communications Manager. The other identity headers such as PPI, RPID, or From are not considered for call anchoring.
- **Trust None**—None of the calls are anchored even if the DN or DURI of a configured remote destinations on the Unified Communications Manager matches any of Identity headers.

For more information on configuring SIP trunks to distinguish between trusted and untrusted identity, see the *Cisco Unified Administration CM Administration Online Help*.

Configure Exchange 2016 as a Presence Gateway over Exchange Web Services

If the connection to the Microsoft Exchange server is over IPv6, ensure that the enterprise parameter is configured for IPv6 and that Eth0 is set for IPv6 on each IM and Presence Service node in the deployment. For information about configuring IPv6 on IM and Presence Service, see the Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager.

To configure exchange 2016 as a Presence Gateway over Exchange Web Services perform the following tasks:

Before you begin

Before you configure a Presence Gateway, you must upload a valid certificate chain to the IM and Presence Service.

Procedure

Step 1 Log in to the Cisco Unified CM IM and Presence Administration user interface.

Step 2 Choose Presence > Gateways.

Step 3 Click Add New.

Step 4 Choose Exchange -- EWS Server for the Presence Gateway Type. For configuration changes to take effect, you must restart the Cisco Presence Engine after you add, update, or delete one or more EWS servers. If you

add multiple EWS servers one after another, you can restart the Cisco Presence Engine once to effect all your changes simultaneously.

Step 5 Enter a meaningful description in the Description field that helps you to distinguish between Presence Gateway instances when you have configured more than one type of gateway.

Step 6 For the Presence Gateway field, enter the server location for the Presence Gateway and ensure that it matches the Subject Common Name (CN) or is present in the Subject Alternative Name field of the Exchange Server certificate. One of these values must be used to connect with the Exchange Server:

- FQDN
- IP address

Note To configure a Presence Gateway for use with a Wildcard Certificate, the node location value that you specify must be part of the subdomain that is protected by the Wildcard Certificate. For example, if a Wildcard Certificate protects the subdomain *.imp.cisco.com, you must enter a node value of server_name.imp.cisco.com in the Presence Gateway field.

If you enter a FQDN, it must match the Subject Common Name (CN) or match one of the protected hosts in the Subject Alternative Name field on the Exchange Server leaf certificate in the certificate chain. The FQDN must resolve to the address that services the request and uses the certificate.

For IPv6, the IPv6 address you enter must match the value that is entered in the SAN field of the Exchange Server certificate.

Step 7 Enter the name of the Impersonation account that the IM and Presence Service uses to connect to the Exchange Server, either in the form of a User Principal Name (for example, user@domain), or a Down-Level Logon Name (for example, domain\user).

Step 8 Enter the Exchange Account Password required for the IM and Presence Service to connect to the Exchange Server. Enter the password again to confirm it. This value must match the Account Password of the previously configured account on the Exchange Server.

Step 9 Enter the port that is used to connect with the Exchange Server. The IM and Presence Service integration with Exchange occurs over a secure HTTP connection. Cisco recommends that you use port 443 (default port) and not change to other ports.

Step 10 Click Save.

Step 11 Confirm the Exchange Server status is showing green for:

- Exchange Reachability (pingable)
- Exchange SSL Connection/Certification Verification

Deprecated Phone Models

The following table lists all the phone models that are deprecated for this release of Cisco Unified Communications Manager, along with the Unified CM release where the phone model first became deprecated. For example, a phone model that was first deprecated in Release 11.5(1) is deprecated for all later releases, including all 12.x releases.

If you are upgrading to the current release of Cisco Unified Communications Manager and you have any of these phone models deployed, the phone will not work after the upgrade.

Table 4: Deprecated Phone Models for this Release

Deprecated Phone Models for this Release	First Deprecated as of Unified CM...
• Cisco Unified Wireless IP Phone 7921 • Cisco Unified IP Phone 7970 • Cisco Unified IP Phone 7971	12.0(1) and later releases
• 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	11.5(1) and later releases

For additional information, refer to *Field Notice: Cisco Unified Communications Manager Release 11.5(x) does not support some deprecated phone models* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/rel_notes/11_5_1/fieldNotice/cucm_b_fn-deprecated-phone-models-1151.html.

For additional information refer to the Field Notice: *Cisco Unified Communications Manager Release 12.0(x) does not support some deprecated phone models* at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/rel_notes/12_0_1/deprecated_phones/cucm_b_deprecated-phone-models-for-1201.html.

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 this release.
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 following methods to migrate from older model to newer model phones:

- Migration FX tool

5. Once all the phones in your network are supported by this release, upgrade your system.

Note Deprecated phones can also be removed after the upgrade. When the administrator logs in to 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 Unified Communications Manager version, and the deprecated phone fails to register.

Emergency Notifications Paging

With this release, the Emergency Notifications Paging feature is updated.

For more information about configuring Cisco Paging Server, see the "Paging" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

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

Enhanced CTL and ITL Phone Trust and Migration

From this release, delivers the enhanced trust relationship with End Points by introduction of long lived ITL Recovery key as signer for the Identity Trust List (ITL) and Tokenless Certificate Trust List (CTL).

This feature has the following benefits:

- Reduce the administrative overhead to manage the phones that lose trust with Cisco Unified Communications Manager for operations, such as change in hostname or regeneration of certificates.
- Improve the phone migration experience from one cluster to another cluster. This is done by creating long-term trust between the phones and the Cisco Unified Communications Manager cluster by one time provisioning. This makes it easier to migrate phones between clusters.

For details on how to migrate phones from one cluster to another cluster, see the Migrate Phones from One Cluster to Another Cluster, on page 23 procedure.

Security Guide Updates

The *Security Guide for Cisco Unified Communications Manager* is updated with the following new topics.

SAST Roles of CTL File

Note *Signer, mentioned in the following table, is used to sign the CTL file.

Table 5: System Administrator Security Token (SAST) Roles of CTL File

Cisco Unified Communications Manager Version	SAST Roles in Token-based CTL File	SAST Roles in Tokenless CTL File
12.0(1)	Token 1 (Signer) Token 2 ITLRecovery CallManager	ITLRecovery (Signer) CallManager
11.5(x)	Token 1 (Signer) Token 2 ITLRecovery CallManager	CallManager (Signer) ITLRecovery
10.5(2)	Token 1 (Signer) Token 2	CallManager (Signer) ITLRecovery
10.5(1) (Not supported)	Token 1 (Signer) Token 2	CallManager (Signer)
10.0(1) (Not supported)	Token 1 (Signer) Token 2	CallManager (Signer)
9.1(2)	Token 1 (Signer) Token 2	Not applicable

Migrate Phones from One Cluster to Another Cluster

Use the following procedure to migrate phones from one cluster to another. For example, from cluster 1 to cluster 2.

Procedure

Step 1 On cluster 2, from Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Find**.

Step 3 From the list of Certificates, click the ITLRecovery certificate and click either **Download .PEM File** or **Download .DER File** to download the certificate in one of the file formats to your computer.
The details of certificate appear.

Step 4 From the list of Certificates, click the CallManager certificate and click either **Download .PEM File** or **Download .DER File** to download the certificate in one of the file formats to your computer.
The details of certificate appear.

Step 5 On cluster 1, from Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 6 Click **Upload Certificate Chain** to upload the downloaded certificate.

Step 7 From the **Certificate Purpose** drop-down list, choose **Phone-SAST-trust**.

Step 8 For the **Upload File** field, click **Choose File**, browse to the ITLRecovery file that you downloaded in Step 3, and then click **Upload File**.

The uploaded ITLRecovery file appears for the **Phone-SAST-Trust** certificate on **Certificate List** window of cluster 1. If the new ITL file has a ITLRecovery certificate for cluster 2, run the command `show itl`.

Step 9 If the phones in cluster 1 have Locally Significant Certificates (LSC), then the CAPF certificate from cluster 1 has to be uploaded in the CAPF-trust store of cluster 2.

Step 10 (Optional) This step is applicable only if the cluster is in mixed mode. Run the **utils ctl update CTLFile** command on the CLI to regenerate the CTL file on cluster 1.

Note
- Run the `show ctl` CLI command to ensure that the ITLRecovery certificate and CallManager certificate of cluster 2 are included in the CTL file with the role as SAST.
- Ensure that the phones have received the new CTL and ITL files. The updated CTL file has the ITLRecovery certificate of cluster 2.

The phones that you want to migrate from cluster 1 to cluster 2 will now accept the ITLRecovery certificate of cluster 2.

Step 11 Migrate the phone from one cluster to another.

Migration from eToken-based CTL File to Tokenless CTL File

For the tokenless CTL file, administrators must ensure that the endpoints download the uploaded CTL file generated using USB tokens on Unified Communications Manager Release 12.0(1) or later. After the download, they can switch to tokenless CTL file. Then, they can run the `utils ctl upgrade` CLI command.

Bulk Certificate Export

Following note is added to this topic.

Note During bulk certificate import, you need to import an additional ITLRecovery certificate on both the visiting cluster and the home cluster for Cisco Extension Mobility Cross Cluster (EMCC) to continue functioning. A new option to import ITL_Recovery certificate is added in Bulk Certificate Management for the **Certificate Type** drop-down list.

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.

External Database Cleanup Utility for IM and Presence

The External Database Cleanup Utility makes it easy for administrators to manage external database growth, thereby ensuring that your system continues to perform at the optimum level. The utility lets you create jobs that monitor the external database on an ongoing basis, deleting old records automatically as they expire. This ensures that the external database has adequate space and that system performance is not impacted by unchecked database growth.

The External Database Cleanup Utility can be used to manage external database growth for the following IM and Presence Service features, each of which relies on the external database:

- Persistent Chat High Availability
- Managed File Transfer
- Message Archiver

Interactions

The following interactions apply:

- Records that are deleted from the database are deleted without archiving.
- You can run the Database Cleanup utility in offline mode.

- A persistent chat room configuration option is provided to override the cluster-wide setting for retention durations. This allows chat room owners to customize the settings within a controlled range. This is dependent on Jabber client changes to enable this menu option.

Using the External Database Cleanup Utility

For information on how to use the External Database Cleanup Utility, refer to the "External Database Administration" chapter of the *External Database Setup Guide for the IM and Presence Service, Release 12.0(1)*.

External Database Text Conferencing Report

The IM and Presence Service now includes the External Database Text Conferencing Report. This report, which can be accessed from the Group Chat and Persistent Chat Settings window, helps you manage the persistent chat rooms in your deployment. You can use this report to view details such as number of chat rooms, number of records per room, and the last time stamp for each room.

This report is supported for all database versions that support persistent chat.

User Interface Updates for External Database Text Conferencing Report

You can access the External Database Text Conferencing Report from the Group Chat and Persistent Chat Settings window by clicking the **Report** button, which is new for this release.

Extension Mobility Roaming Across Clusters

Note To deploy Extension Mobility Roaming Across Clusters, you must be running a minimum release of 12.0(1)SU1.

Extension Mobility Roaming Across Clusters allows users to roam across multiple clusters and make or receive calls even when the user's home cluster is down. This feature uses the Inter-cluster Lookup Service (ILS) to replicate Extension Mobility users' directory numbers and log in information across the ILS network.

When a provisioned user logs in to a remote cluster, their phone registers to the remote cluster using the directory number and user information from the home cluster. Unlike Extension Mobility Cross Cluster (EMCC), where the phone from the visiting cluster registers to the home cluster, the roaming feature allows the user to maintain their registration in whichever cluster they visit. This roaming feature allows users to maintain a single set of log in credentials across the ILS network.

Extension Mobility Roaming Across Clusters Prerequisites

Extension Mobility roaming across clusters has the following prerequisites:

- You must set up an ILS Network. For more information about configuring ILS, see the Configure Intercluster Lookup Service chapter in the *System Configuration Guide for Cisco Unified communications Manager* at https: %20 www.cisco.com c en us support unified-communications unified-communications-manager-callmanager %20products-installation-and-configuration-guides-list.html.

- All clusters must have a uniform dial plan. To set up a dial plan, see the Configure the Dial Plan chapter in the *System Configuration Guide for Cisco Unified Communications Manager* at https: %20 www.cisco.com c en us support unified-communications unified-communications-manager-callmanager %20products-installation-and-configuration-guides-list.html.

For more information, see the Extension Mobility Roaming Across Clusters chapter in the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Home Cluster Routing Through Session Management Edition for Cisco Spark Hybrid Call Service Connect

In this release, Session Management Edition (SME) can route calls for Cisco Spark Hybrid Call Service Connect to the home cluster of the calling user before it reaches the destination. In the earlier releases, these calls were routed directly to the home cluster by Expressway-Core (Expressway-C).

Use this feature to enable SME to centralize routing in a Cisco Hybrid Call Service Connect deployment. By using SME:

- You do not require full mesh deployment of SIP trunks from ingress Expressway-C to leaf Cisco Unified Communications Manager clusters. Without SME, you require such deployment.
- The routing, which is based on route headers, is partially compliant with RFC 3261.

For smaller deployments, an Expressway-C is configured with a direct SIP trunk to every Cisco Unified Communications Manager cluster. However, for larger deployments with multiple Cisco Unified Communications Manager clusters, SME is deployed to simplify intercluster routing. By using this feature, an administrator can configure SIP trunks from Expressway-Cs to SMEs and from SMEs to Cisco Unified Communications Manager clusters.

For more information, see the Hybrid Call Service Connect documentation at http://www.cisco.com/go/hybrid-services.

Call Flow

Following is the call flow for home cluster routing for SME from Cisco Spark to Cisco Unified Communications Manager.

Before you begin

- Configure Expressway-C to route to SME and to pass the route headers.

Procedure

Step 1 For caller A, Cisco Spark includes the Cluster Fully Qualified Domain Name (CFQDN) of caller A's Unified Communications Manager cluster in the route header and request Uniform Resource Identifier (URI) of called party B.

Step 2 Call is routed to SME and the route headers are passed in INVITE to SME.

Step 3 SME routes the call to the leaf cluster that is identified in the Route header. The leaf cluster removes the route header and passes the request URI of called party B.

Step 4 The leaf cluster routes the call according to the request URI.

Note Depending on the leaf cluster routing configuration, the call may be terminated to a local device or forwarded through a SIP trunk. Hence, the call may go back to SME. However, this routing does not happen as part of this feature.

IPv6-only Network

Note The IPv6-only feature is dependent on having the latest phone firmware loads that are tested and supported with Cisco Collaboration Systems Release 12.0. The CSR-12.0 supported phone loads are expected to be released in September 2017. For details on supported loads with Collaboration Systems Release 12.0, see http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/CSR-Compatibility-Matrix-InteractiveHTML.html.

With this release, Cisco Unified Communications Manager supports IPv6-only SIP networks for endpoints. This allows you to deploy your endpoints in an IPv6-only configuration. IPv6 provides a much broader range of IP addresses than IPv4, which greatly reduces the risk of IP address exhaustion. In addition, IPv6 also provides the following additional benefits:

- Stateless address autoconfiguration
- Simplified multicasting functionality
- Simplified routing, minimizing the need for routing tables
- Delivery of services optimization
- Better handling of mobility
- Greater privacy and security

To facilitate IPv6-only support, the following system components and features have been updated in this release to support IPv6 addresses:

- Device Mobility
- NTP
- SRST
- SNMP
- Web Dialer
- Extension Mobility
- Self Care Portal
- Self Provisioning (with or without IVR)

- Barge, Intercom
- EnergyWise power save mode
- IPv6-only SIP gateway

Note If you are deploying an IPv6-only network for SIP endpoints, the Cisco Unified Communications Manager server will use both an IPv4 and IPv6 address due to the fact that some internal system components and applications support IPv4 only. However, endpoints can operate with IPv6 addressing only.

Note To deploy the Cisco Unified Communications Manager 12.0(1) for the IPv6-only support, install the phone load 12.0(1) COP files in the cluster nodes and restart the TFTP services and phones as required.

Configure IPv6

For details on how to configure the IPv6 stack, see the "Configure IPv6" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*.

IPv6 Support for Device Mobility

With this release, Cisco Unified Communications Manager provides IPv6 support for the Device Mobility feature. Device mobility allows mobile users to roam from one site to another and acquire settings that are specific to that site. Your system then uses these dynamically allocated settings for functions such as call routing, codec selection, and media resources.

Previously, device mobility was available in IPv4 only. The addition of IPv6 support for this feature helps you to deploy your network with IPv6-only endpoints. For more information about the configuration, see the “Device Mobility” chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager*.

User Interface Updates for IPv6 Support

In the **Device Mobility Info Configuration** window, a new **IPv6 Subnet** section is added with the following fields:

- **Subnet**—You can enter the device mobility IPv6 subnet address in the colon-separated hexadecimal format.
- **Mask Size**—You can enter the device mobility subnet mask for IPv6 address.

IPv6 Support for NTP Reference and SRST Settings

With this release, Cisco Unified Communications Manager provides IPv6 support for NTP Reference and SRST settings. Previously, these components supported IPv4 addresses only. This support allows you to deploy your network with IPv6-only endpoints.

User Interface Updates for IPv6 Support

The following configuration windows have been updated with new fields for IPv6 support:

- Phone NTP Reference Configuration window—an **IPv6 Address** field is added to specify an IPv6 address for the NTP server.
- SRST Reference Configuration window—a **SIP Network/IPV6 Address** field is added to specify an IPv6 address of the server that the phones that are running SIP uses when in SRST mode.

IPv6 Support for Simple Network Management Protocol (SNMP)

With this release, Cisco Unified Serviceability provides IPv6 support for SNMP V1/V2c and V3 setup. Previously, these components supported IPv4 addresses only. This support allows you to deploy your network with IPv6-only endpoints.

User Interface Updates for IPv6 Support

In the following configuration windows, the **Host IP Addresses** field is renamed to **Host IPv4/IPv6 Addresses** and the **Host IP Address** field is renamed to **Host IPv4/IPv6 Address**.

- SNMP Community String Configuration
- SNMP Notification Destination Configuration
- SNMP User Configuration

You can enter specific IPv6 address in the **Host IPv4/IPv6 Address** field to accept SNMP packets only from that particular address.

CLI Command Updates for IPv6 Support

The following SNMP commands now support IPv6 address:

- **utils snmp get**
- **utils snmp get 1**
- **utils snmp get 2c**
- **utils snmp get 3**
- **utils snmp walk**
- **utils snmp walk 1**
- **utils snmp walk 2c**
- **utils snmp walk 3**

IPv6 Support for Web Dialer

With this release, Cisco Unified Communications Manager provides IPv6 support for Cisco Web Dialer Web Service. Previously, these components supported IPv4 addresses only. This support allows you to deploy your

network with IPv6-only endpoints. For more information about the configuration, see the "Web Dialer" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Independent Audio and Video Bit Rates for Video Calls

In this release, the Regions Configuration feature allows you to split the maximum bit rate calculations for the audio and video streams of a video call. When you configure this feature, the maximum bit rate calculation for a video call includes only the video portion. However, the audio portion appears in an existing field. In the previous releases, the maximum bit rate for a video call included both the audio and video streams.

This feature makes the calculation of Locations-based Call Admission Control for video calls easier by making the audio and video bandwidth splits more transparent. You can view the call admission details, such as the number of calls which can be admitted with audio and video independently. The call admission is based on the aggregate bandwidth that is available for audio and video calls within or between regions.

You can enable this feature by configuring the **Deduct Audio Bandwidth Portion from Audio Pool for a Video Call** service parameter to **True**.

Configure Video Calls to Split the Audio and Video Bandwidth

Use the following procedure to configure the system to split the audio and video bandwidth allocations for video calls into separate audio and video pools. The default configuration for video calls is to deduct both the audio and video bandwidth allocations from the video pool.

Procedure

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

Step 2 From the **Server** drop-down list, choose the publisher node.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 Configure the **Deduct Audio Bandwidth Portion from Audio Pool for a Video Call** service parameter to **True**.

Note When you configure this service parameter to **True**, the video and immersive video parameters are considered as media level and not as session level. Hence, for a video call, you can allocate audio and video bandwidths from audio and video pools respectively for each region and location. The video and immersive video bandwidth limits apply only to the video media stream; not to the combination of the audio and video media streams.

Step 5 Click **Save**.

User Interface Updates

Following updates have been done for this feature.

Service Parameter Updates

Previously, the **Deduct Audio Bandwidth Portion from Audio Pool for a Video Call** service parameter covered only the audio and video splits in the Call Admission Control bandwidth deductions for a video call. With this release, this service parameter configuration also specifies the split in the Regions maximum bit rate calculation for a video call. For Regions calculation, you can configure one of the following values:

- **True**—When you configure this value, the maximum bit rate allowance for a video call includes the video stream only. A video call includes both regular video and immersive video.
- **False** (default setting)—When you configure this value, the maximum bit rate allowance for a video call includes both the audio and video streams. A video call includes both regular video and immersive video.

Regions Configuration Updates

Based on the value you choose for the **Deduct Audio Bandwidth Portion from Audio Pool for a Video Call** service parameter, changes in the following fields of the **Region Configuration** window appear:

- **Maximum Session Bit Rate for Video Calls**—If you configure the service parameter to **True**, this field is renamed to **Maximum Video Bit Rate for Video Calls** and includes the video bit rate only. The audio portion is calculated in the existing **Maximum Audio Bit Rate** field.
- **Maximum Session Bit Rate for Immersive Video Calls**—If you configure the service parameter to **True**, this field is renamed to **Maximum Video Bit Rate for Immersive Video Calls** and includes the video bit rate only.

Note These changes are applicable for both the **Region Relationships** and the **Modify Region Relationship to other Regions** sections of the **Region Configuration** window.

Location Configuration Updates

Based on the value you choose for the **Deduct Audio Bandwidth Portion from Audio Pool for a Video Call** service parameter, changes in the following fields of the **Locations Configuration** window appear:

- **Session Bandwidth in Video Calls**—If you configure the service parameter to **True**, this field is renamed to **Video Bandwidth for Video Calls** and includes the video bit rate only.
- **Session Bandwidth for Immersive Video Calls**—If you configure the service parameter to **True**, this field is renamed to **Video Bandwidth for Immersive Video Calls** and includes the video bit rate only.

When you click **Add**, the pop-up window shows the same fields for the links of bandwidth between two or more locations section, as shown in the **Location Configuration** window.

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 34 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.

set tls min-version

This command sets the minimum version of Transport Layer Security (TLS) protocol.

Note

- After you set the minimum TLS version, the system reboots.
- Configure the minimum TLS version for each node.

set tls min-version *tls minVersion*

Syntax Description

Parameters	Description
tls minVersion	Type one of the following options to set it as the minimum TLS version: • 1.0 • 1.1 • 1.2

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Prime License Manager

Example

```
admin: set tls min-version 1.1

This command will result in setting minimum TLS version to 1.1 on all the secure interfaces.
If you have custom applications that makes secure connection to the system, please ensure
they support the TLS version you have chosen to configure.
Also, please refer to the Cisco Unified Reporting Administration Guide to ensure the
```

```
endpoints in your deployment supports this feature.

************************************************************************************************

Warning: This will set the minimum TLS to 1.1 and the server will reboot.

************************************************************************************************

Do you want to continue (yes/no) ? yes

Successfully set minimum TLS version to 1.1

The system will reboot in few minutes.
```

show tls min-version

This command shows the minimum configured version of Transport Layer Security (TLS) protocol.

show tls min-version

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Prime License Manager

Example

```
admin:show tls min-version
Configured TLS minimum version: 1.0
```

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.

Mobile and Remote Access Policy for Jabber

Note The Mobile and Remote Access (MRA) Access Policy is not yet supported. Full support will be added with a future release of Cisco Jabber. The feature is available in this release of Cisco Unified Communications Manager for preview only. We recommend that you do not turn this feature on until Jabber support is added.

With this release, you can set up a policy in Cisco Unified Communications Manager to provision Mobile and Remote Access (MRA) feature access for Cisco Jabber users. The MRA Access Policy allows you to

specify the types of Jabber services that Jabber users can access over MRA. This feature is applicable only for Jabber MRA users and not applicable to any other endpoints or clients.

Expressway applies the policy only to those clients that use OAuth code flow. Expressway does not restrict access for clients that use other authentication methods. However, only clients that use OAuth code flows can have their access levels managed through the MRA Access Policy.

Mobile and Remote Access feature involves configurations on Cisco Unified Communications Manager and compatible versions of Cisco Expressway and Cisco Jabber.

For Cisco Unified Communications Manager set up, see the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

For Expressway set up, see http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.

This feature is supported on Cisco Unified Communications Manager only when it is deployed with compatible versions of Cisco Jabber and Cisco Expressway, which also support this feature. Refer to the Cisco Jabber and Cisco Expressway release notes for confirmation on the availability of this feature.

User Interface Updates

To support this feature, **Mobile and Remote Access Policy** section and **Jabber Policies** section has been added to the **User Profile Configuration** window.

The **Mobile and Remote Access Policy** section consists the **Enable Mobile and Remote Access** check box. This check box enables a user with this user profile to register with the MRA feature over Expressway.

The **Jabber Policies** section consists the following fields:

- **Jabber Desktop Client Policy**—This policy specifies the Jabber services that are available to Cisco Jabber for Windows users and Cisco Jabber for Mac users who are associated to this user profile
- **Jabber Mobile Client Policy**—This policy specifies the Jabber services that are available to Cisco Jabber for iPhone or iPad users and Cisco Jabber for Android users who are associated to this user profile

The available policies options for the **Jabber Desktop Client Policy**, or the **Jabber Mobile Client Policy** is:

- No Service—This policy disables access to all Jabber services
- IM & Presence only—This policy enables only instant messaging and presence capabilities
- IM & Presence, Voice and Video calls—This policy enables instant messaging, presence, voicemail, and conferencing capabilities for all users with audio or video devices. This is the default option

New Certificate Added to the Trust Store

The Adaptive Security Appliance (ASA) Transport Layer Security (TLS) proxy functionality requires Change and Configuration Management (CCM) Proxy certificates to be available in the Certificate Trust List (CTL) file. This enables phones initiating a TLS connection to ASA to trust the certificate offered by ASA.

An ASA certificate could be only added to a CTL file by CTL client. As of release 12.0.1, system administrators can add an ASA certificate using tokenless CTL through CTL CLI. A new certificate has been added to the trust store to enable ASA TLS proxy to work with Cisco Unified Communications Manager.

User Interface Updates

A new certificate **Phone-CTL-ASA-trust** is added to the **Certificate Purpose** drop-down menu in **Cisco Unified OS Administration > Security > Certificate Management > Certificate List** screen > **Upload Certificate/Certificate chain** button > **Upload Certificate/Certificate chain** screen.

System administrators can download the ASA certificate and upload it in the **Upload Certificate/Certificate chain** screen. After the ASA certificate is imported to **Phone-CTL-ASA-trust**, administrators need to regenerate CTL file using any of the following CLI commands to include the imported certificate in the CTL file:

- `utils ctl set-cluster mixed-mode`
- `utils ctl update CTLFile`

New Columns to Manage Devices Efficiently

In certain scenarios, Cisco Unified Communications Manager upgrades and other administrative actions caused Session Initiation Protocol (SIP) or Skinny Client Control Protocol (SCCP) endpoints to unregister from Cisco Unified Communications Manager. The unregistered phones were not registered on Cisco Unified Communications Manager again. As a result, administrators were unable to identify the unregistered endpoints.

As of Release 12.0.1, Cisco Unified Communications Manager displays the phones that were unregistered, unused, and active. Administrators can track when an unregistered phone was last registered and when a registered phone was last active. This feature enables an administrator to track phones effectively, even when a phone is unregistered from Cisco Unified Communications Manager.

The endpoints that support this feature are SIP phones such as Cisco Jabber and SCCP phones. The endpoints that do not support this feature are Computer Telephony Integration (CTI), Media Gateway Control Protocol, H323, virtual endpoints, and phones logged in through extension mobility cross cluster.

This feature is enabled by default. Administrators can choose to enable or disable this feature in the **Service Parameter Configuration** screen at **System** > **Service Parameters** . The **Phone Status Update Window** parameter of the **Cisco Database Layer Monitor (Active)** service can be assigned values from 0 to 24 hours.

- This feature is enabled by default and 12 hours is the default value. The feature remains enabled when an administrator sets a value from 1 to 24 hours. After an upgrade or a migration from pre 12.0.1 to 12.0.1 or above, the default value changes to 12 hours only if it is less than 12 hours in the previous version. If the value in the previous version is 12 hours or above, it remains the same.

  If there is a reboot of the node or a restart of the Cisco Call Manager Service during the Phone Status Update Window, only the end points which are supposed to be updated or already updated during the time period keepalive Interval * 10 will be updated again. For example, if DB maintenance Time is 00:00 and Phone Status Update Window is 12 hours and the Call Manager after restart comes back at 08:00, keepalive interval is 2 minutes, then the phones which had to be updated 20 minutes before 08:00 will be updated again. For SCCP phones the Station KeepAlive Interval Service parameter is considered.

- This feature is disabled when an administrator sets the value to 0.

User Interface Updates

The **Find And List Phones** screen in Cisco Unified Communications Manager has been enhanced to track phones efficiently. The **Find And List Phones** screen is at:

- **Device** > **Phone**
- **Bulk Administration** > **Phones** > **Update Phones** > **Query**
- **Bulk Administration** > **Phones** > **Delete Phones** > **Query**
- **Bulk Administration** > **Phones** > **Export Phones** > **Query**

The **Find And List Phones** screen in Cisco Unified Communications Manager has been enhanced in the following ways:

- The following columns have been added:
  - **Last Registered**: Displays the timestamp when an **Unregistered** device was last registered. The timestamp is displayed in the format MM/DD/YYYY HH:MM and the time is displayed in the local time format.
  - **Last Active**: Displays the timestamp when a device was last actively involved in a call. The timestamp is displayed in the format MM/DD/YYYY HH:MM and the time is displayed in the local time format.
  - **Unified CM**: Displays the host name or the IP address of the server for both registered and unregistered devices.

  If this feature is disabled, the **Last Registered** and the **Last Active** columns display Not Applicable for unregistered phones and the Unified CM column is blank.
- The data displayed in the **Status** column before version 12.0.1 is now displayed across two columns **Status** and **Unified CM**.
  - The **Status** column now displays only the status of the device. The status of a device can be Unregistered, Registered, Unknown, None or Rejected.
  - The **Unified CM** column displays the hostname or IP address of the server on which device is registered or unregistered.
- The following values have been added to the **Find Phone Where** filter:
  - **Last Registered**: Displays the unregistered devices in the specified time frame. Administrators can apply this filter to view only the devices that are not currently registered. Administrators can
    1. Select **Last Registered**.
    2. Specify **Before** or **After**.
    3. Specify a required timestamp in the format MM/DD/YYYY HH:MM or MM/DD/YYYY.
    4. Click **Find**.
  - **Last Active**: Displays the devices that were active during a specified time frame. Administrators can
    1. Select **Last Registered**.
    2. Specify **Before** or **After**.
    3. Specify a required timestamp in the format MM/DD/YYYY HH:MM or MM/DD/YYYY.
    4. Click **Find**.

The **Last Registered**and**Last Active** filters can be applied only when this feature is enabled.

New Sign-In Options for Extension Mobility Users

The extension mobility feature allows users to temporarily access their phone settings, such as line appearances, services, and speed dials, from other phones within their system. The extension mobility cross cluster (EMCC) feature provides users with the same functionality as extension mobility, but also allows them to move from one cluster (the home cluster) and sign-in to a temporary phone on another remote cluster (the visiting cluster).

As of Release 12.0.1, administrators can configure more sign-in options for IP phone users who have subscribed to the extension mobility or extension mobility cross cluster services. In addition to signing in using User ID and PIN, administrators can now allow users to sign-in using any of the following credentials:

- Primary Extension and PIN
- Self Service User ID and PIN

This enables users to sign-in to IP phones easily and avoid entering lengthy User IDs containing alphanumeric and special characters using a telephone keypad. For example, john2.doe@us.example.com

For the new sign-in options to work seamlessly with EMCC, ensure that the home and visiting clusters are upgraded to Cisco Unified Communications Manager release 12.0.1.

New Parameters to Configure Sign-In Options

Administrators can configure more sign-in options by adding a new parameter `loginType` to the Service URL of the device. Administrators can select **Device** > **Device Settings** > **Phone Services** > **IP Phone Services Configuration**, and append `loginType` to the end of the URL in the **Service URL** field. Administrators can configure the following:

- `loginType=DN` to enable users to sign-in using Primary Extension and PIN

  The Service URL format is: `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#&loginType=DN`

- `loginType=SP` to enable users to sign-in using Self Service User ID and PIN

  The Service URL format is: `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#&loginType=SP`

- `loginType=UID` to enable users to sign-in using User ID and PIN

  The Service URL format is: `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#&loginType=UID`.

If administrators do not append `loginType` to the end of the URL, the default sign-in option displayed is User ID and PIN.

Non-compliance to FIPS

Unified Communications Manager Release 12.0 is non-FIPS compliant.

We recommend that you disable FIPS mode before you upgrade to a non-FIPS compliant release of Unified Communications Manager or upgrade to the next FIPS-compliant release. The next available FIPS-compliant release is Unified Communications Manager Release 12.5SU1.

IPsec Requirements

With this release, the Libreswan library support replaces Openswan library support for IPsec. This support has no changes to the existing functionality.

For the certificate-based authentication to function with the Libreswan library, the certificates of both the source and destination must be CA-signed certificates. In addition, same certificate authority (CA) must sign these certificates. The migration to the Libreswan library has the following limitations:

- IPsec stops working if you're using certificate-based authentication and self-signed certificates for setting up IPsec.
- IPsec stops working if you're using certificate-based authentication and CA-signed certificates with different CAs signing source and destination for setting up IPsec.

Security Guide Updates

For the Openswan to Libreswan migration for IPsec feature, following updates have been made in the *Security Guide for Cisco Unified Communications Manager*.

- All the instances of Openswan have been replaced with Libreswan.
- A note on the unsupported algorithms has been added.

SAML SSO Support for Cisco Unified Communications Manager Web Interfaces

With this release, the Cisco Unified OS Administration and Disaster Recovery System are now the Security Assertion Markup Language (SAML) SSO-supported applications. If SAML SSO is enabled, you can launch these applications or other supported applications, such as Cisco Unified Communications Manager, after a single sign-in with an Identity Provider (IdP). You no longer need to sign in to these applications separately.

To support SAML SSO for Cisco Unified OS Administration and Disaster Recovery System, the Level 4 administrator creates the Level 0 and Level 1 administrators in the active directory. The Level 4 administrator adds the platform administrators in all the nodes of a cluster. With this addition, the platform administrators are synchronized between the active directory and the platform database. While configuring users in platform database, the administrator must configure the **uid** value for the user. Cisco Unified OS Administration and Disaster Recovery System applications use the **uid** value to authorize a user. The IdP server authenticates their credentials against the active directory server and sends a SAML response. After authentication, Cisco Unified Communications Manager authorizes the users from the platform database using the **uid** value. For details on **uid** value, see Configure Unique Identification Value for Platform Users, on page 41 procedure.

If SAML SSO is enabled for the existing release and you upgrade from earlier release to the new release, the SAML SSO support is available for Cisco Unified OS Administration and Disaster Recovery System applications in the new release. The SAML SSO support for these applications is also enabled when you

enable SAML SSO for any Cisco Unified Communications Manager web applications. To enable the SAML SSO support for the new release, see the SAML SSO Enablement topic from the *SAML SSO Deployment Guide for Cisco Unified Communications Applications* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Note When SAML SSO support is enabled for a Cisco Unified Communications Manager administrator, it is applicable across the cluster. However, for the Cisco Unified OS Administration and Disaster Recovery System applications, each platform administrator is specific to a node and these user details are not replicated across the cluster. So, each platform user is created in each subscriber node of a cluster.

Configure Unique Identification Value for Platform Users

The unique identification (UID) value is used to authorize a platform user to do SSO login on platform pages. The Level 4 administrator can configure this value for platform administrators in one of the following ways:

- While creating the platform users by using the **set account name** command on the CLI. For details, see the set account name, on page 41 topic.
- While updating the existing **uid** value. For details, see the set account ssouidvalue, on page 42 topic.

CLI Reference Guide Updates

The *Set Commands* chapter from the *CLI Reference Guide for Cisco Unified Communications Solutions* is updated with the following new and enhanced CLI commands for the SAML SSO support for Cisco Unified OS Administration and Disaster Recovery System feature.

Enhanced CLI Command

set account name

The **set account name** command is enhanced with the following newly added prompts:

- **Allow this User to login to SAML SSO-enabled system through Recovery URL ? (Yes / No)**—Level 4 administrator can enable or disable the access to the recovery URL sign-in option for new platform administrators by typing **Yes** or **No** on the CLI. The value can be configured to **Yes** if a user chooses to sign-in using the Recovery URL.
- **To authenticate a platform login for SSO, a Unique Identifier (UID) must be provided that identifies this user to LDAP (such as sAMAccountName or UPN). Please enter the appropriate LDAP Unique Identifier (UID) for this user:[UID]**—Level 4 administrator can type the unique identifier value for each platform administrator for this prompt.

Note Only the Level 4 administrator has privileges to run all the CLI commands.

Note The administrator must ensure to perform the following tasks:

- Type either **Yes** or **No** for the **Allow this User to login to SAML SSO-enabled system through Recovery URL ? (Yes / No)** prompt. If this prompt value is blank, an error message appears.
- Type a value for the **To authenticate a platform login for SSO, a Unique Identifier (UID) must be provided that identifies this user to LDAP (such as sAMAccountName or UPN). Please enter the appropriate LDAP Unique Identifier (UID) for this user:[UID]** prompt. If the prompt value is duplicate, an error message appears. You can hit the Enter key and then, the user account name is saved by default.

New CLI Commands

set account ssouidvalue

This command updates the unique identifier value for the existing platform administrators.

set account ssouidvalue *userid*

Syntax Description

Parameters	Description
userid	Specifies a particular Cisco Unified Operating System Administrator account whose unique identifier value needs to be updated.

Command Modes

Administrator (admin:)

Usage Guidelines

Note

- When you run the **set account ssouidvalue userid** command, a prompt appears to provide the UID value. If the UID value is blank, then samaccountname is saved as ssouidvalue by default.
- If a duplicate UID value exists, an error appears.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager

set account ssorecoveryurlaccess

This command enables or disables the SSO recovery URL access for platform administrators.

Note By default, the platform administrator Level 4 has access to the recovery URL. If the platform administrator Level 4 attempts to update the recovery URL access for own self, an error appears.

set account ssorecoveryurlaccess {**enable** | **disable**}*userid*

Syntax Description

Parameters	Description
enable	Enable the recovery sign-in option for platform administrators.
disable	Disable the recovery sign-in option for platform administrators.
userid	Specifies a particular Cisco Unified Operating System Administrator account.

Command Modes

Administrator (admin:)

Usage Guidelines

Note
- If you enable or disable the recovery sign-in option, which is already enabled or disabled, an error appears.
- The administrator account that the system creates when Unified Communications Manager installs has a privilege level of 4. The administrator can run all commands in the CLI.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager

Recovery URL Sign-in Option for Cisco Unified OS Administration

With this release, platform administrators can access Cisco Unified OS Administration either by signing in to one of the SAML SSO-enabled applications or by using the recovery URL option. This option is available as **Recovery URL to bypass Single Sign On** link on the main page of the SSO-enabled nodes. Platform users can sign in to Cisco Unified OS Administration if they have Recovery URL access.

The Level 4 administrator configures the recovery URL sign-in option for platform users. The administrator can enable this option while the platform administrators are being created through CLI or when their details are being updated using the CLI command. For details on the CLI commands for recovery URL login for new and existing platform administrators, see the CLI Reference Guide Updates, on page 41 topic.

Note By default, the **Recovery URL to bypass Single Sign On** link is enabled for the Level 4 administrator. This link is enabled for the platform administrators Level 0 and Level 1 in case of upgrade from earlier release to the new release.

SAML SSO Okta Identity Provider

With this release, the Cisco Unified Communications Manager supports Okta as an Identity Provider for SAML SSO. The Okta has been tested with version 2017.38.

For details on how to configure Cisco Unified Communications Manager for SAML SSO integration with Okta, refer to the *SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 12.0(1)* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/SAML_SSO_deployment_guide/12_0_1/cucm_b_saml-sso-deployment-guide-1201.html .

.

Smart Software Licensing

Cisco Smart Software Manager replaces Prime License Manager in Cisco Unified Communications Manager Release 12.0(1) and later versions. Cisco Prime License Manager is no longer used as of Release 12.0(1) and no longer appears in the Installed Applications pre-login screen.

Cisco Smart Software Licensing is a new way of thinking about licensing. It adds flexibility to your licensing and simplifies it across the enterprise. It also delivers visibility into your license ownership and consumption.

Cisco Smart Software Licensing helps you to procure, deploy, and manage licenses easily where devices self-register and report license consumption, removing the need for product activation keys (PAK). It pools license entitlements in a single account and allows you to move licenses freely through the network, wherever you need them. It is enabled across Cisco products and managed by a direct cloud-based or mediated deployment model.

This service registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

You can use Smart Licensing to:

- Register with Cisco Smart Software Manager or Cisco Smart Software Manager satellite
- See the license usage and count
- See the status of each license type
- See the product licenses available on Cisco Smart Software Manager or Cisco Smart Software Manager satellite
- Renew License Authorization with Cisco Smart Software Manager or Cisco Smart Software Manager satellite
- Renew the License Registration
- Deregister with Cisco Smart Software Manager or Cisco Smart Software Manager satellite

Configuration Details

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

User Interface Updates

To manage this feature, the **License Usage Report** page (**System** > **Licensing**) has been replaced with **License Management** page (**System** > **Licensing**) of the Cisco Unified CM Administration interface.

The License Management page provides the summary and detailed information on the system license usage as it is reported to the Cisco Smart Software Manager or Cisco Smart Software Manager satellite. Licenses are assigned to the company Smart Account and are not node locked to a device.

The following table displays the online help updates for this feature.

Field	Description
Status	The **Status** message displays the steps to register with Cisco Smart Software Manager or Cisco Smart Software Manager satellite and the current license registration mode.
Smart Software Licensing	
Registration Status	Displays the current registration status. The different statuses are: • Registered—For the product which is registered. • Unregistered or Unidentified—For the product which is unregistered. • Unregistered-Registration Expired—For the product which registration is expired.

Field	Description
License Authorization Status	Displays one of the following status information: • Authorized—Product in authorized or in compliance state. • Authorization Expired—Authorization is expired for the product. This usually happens when the product has not communicated with Cisco for 90 continuous days. It is in an overage period for 90-days before enforcing restrictions to set up users and devices. • Out of Compliance—Product is in out of compliance state because of insufficient licenses. It is in an overage period for 90-days before enforcing restrictions to set up users and devices. • No Licenses in Use—There are no licenses being consumed by the product instance. • Evaluation Mode—Product in evaluation mode and not yet registered with Cisco. • Evaluation Period Expired—Evaluation period has expired. • Not Applicable—Unable to determine current registration status.
Export-Controlled Functionality	Specifies if the Export-Controlled functionality was enabled in the token with which the product was registered. **Note** The **Allow export-controlled functionality on the products registered with this token** check box is not displayed for the Smart Accounts that are not permitted to use the Export-Controlled functionality. Displays one of the following status information: • Allowed—The token registered with has Allow export-controlled functionality selected. • Not Allowed—The token registered with do not have Allow export-controlled functionality selected or Cisco Unified Communications Manager not registered.

Field	Description
Transport Settings	The different settings through which Unified Communications Manager can connect to Cisco Smart Software Manager or Cisco Smart Software Manager satellite are: **Note** If you choose to use direct connection, then you must configure Domain Name System (DNS) on Cisco Unified Communications Manager that can resolve https://www.cisco.com. • Direct—Cisco Unified Communications Manager sends usage information directly over the internet. No additional components are needed. • Cisco Smart Software Manager satellite—Cisco Unified Communications Manager sends usage information to an on-premise Smart Software Manager. Periodically, an exchange of information is performed to keep the databases in synchronization. For more information on installation or configuration of the Smart Software Manager satellite, go to this URL: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html. • Proxy Server—Cisco Unified Communications Manager sends usage information over the internet through a proxy server. **Note** If you choose not to configure the domain and Domain Name System (DNS) on Cisco Unified Communications Manager, then you can select the Cisco Smart Software Manager satellite or transport gateway or proxy server under Transport settings. In such case, DNS that can resolve https://www.cisco.com has to be configured on the Cisco Smart Software Manager satellite or proxy server. **Note** If you choose not to use the DNS server in your deployment and not connect to the internet, then you can select the Cisco Smart Software Manager satellite with manual synchronization in disconnected mode.

Field	Description
Smart Account	Displays information of the customer Smart Account. It is created from the **Request a Smart Account** option under **Administration** section of the https://software.cisco.com. It is the primary account created to represent the customer and all licenses for a company are assigned to this Smart Account. It also manages licenses for all Cisco products.
Virtual Account	A self-defined construct to reflect the company organization. Licenses and Product instances can be distributed across virtual accounts. Created and maintained by the administrator on the Cisco Smart Software Manager or Cisco Smart Software Manager satellite with full visibility to company assets.
Register	Use the **Register** button to register Cisco Unified Communications Manager with Cisco Smart Software Manager or Cisco Smart Software Manager satellite. **Note** The **Register** button gets disabled after a successful registration with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.
Actions	The **Actions** drop-down list gets activated only after a successful registration. It lists the following type of actions that can be performed: • Renew Authorization Now • Renew Registration Now • Reregister • Deregister
License Usage Report	
Update Usage Details	The License Usage Report provides the summary and detailed information on the system license usage as it is reported to the Cisco Smart Software Manager or Cisco Smart Software Manager satellite. Usage details are available by license type, users, and unassigned devices. Usage information is updated once every 6 hours, and may be updated manually by clicking on **Update Usage Details**. Clicking Update Usage Details is a resource-intensive process and may take a few minutes depending on the size of your system. There is a link provided to review the Unified Communications licensing information in **View all license type descriptions and device classifications**.

Field	Description
License Requirements by Type	
License Type	The **License Type** column lists the various types of licenses: • Essential • Basic • Enhanced • Enhanced Plus • CUWL • TelePresence Room
Current Usage	The **Current Usage** column shows current license usage (number of licenses required) by license type and summarizes the number of users and unassigned devices that are requiring licenses by license type.
Status	Displays the status of each license type. The different statuses are: • Authorization Expired—The authorized period has expired. • Evaluation—The agent is using the evaluation period for this entitlement. • Evaluation Period Expired—Evaluation period has expired. • Authorized—In compliance (authorized). • No Licenses in Use—There are no licenses being consumed by the product instance. • Invalid—Error condition state. • Invalid Tag - The entitlement tag is invalid. • Not Applicable—Enforcement mode is not applicable. • Out of Compliance—Out of compliance. • Waiting—The initial state after an entitlement request while waiting for the authorization request response.

Field	Description
Report	The Report links by license type are provided by (number of) Users or (number of) Unassigned Devices and allow drill—down links. For the user report, the User ID link provides details on the user configuration per user id. The View Details link provides license requirements per user id. For the Unassigned Devices report, the Device Type and License Type that is required is displayed for each unassigned device.
Users and Unassigned devices	
Users	The Users row lists the total number of users configured on the system. View Usage Report for the users provides a report for all users configured on the system and their corresponding license requirements.
Unassigned Devices	View Usage Report for the Unassigned Devices shows the total number of unassigned devices (devices with no associated user). **Note** Assigning a user ID to a device using Cisco Unified Communications Administration moves the device from "Unassigned Devices" to "Users" in the License Usage Report. However, adding a device to the list of controlled devices for a user does not modify the "License Usage Report" results for the device.
Smart Licensing Product Registration	
This section shows that the Unified Communications Manager licenses are managed by Cisco Smart Software Manager or Cisco Smart Software Manager satellite. It also provides a link to the **Smart Software Manager** page.	

CLI Updates

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

- license smart deregister
- license smart renew auth
- license smart renew ID
- license smart register idtoken <token> [force]
- show license all
- show license status
- show license summary

- show license tech support
- show license trace
- show license UDI
- show license usage

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

Service, Alarm, and Alert Updates

Service

The platform service has been updated to support this feature.

Service Group	Services
Platform Services	Cisco Tomcat and Cisco Smart License Manager

Alarm

The SLMAlarmCatalog has been added to support this feature.

Name	Description
SLMAlarmCatalog	Alarms for Cisco Smart Licensing

The ClusterModeSecurityFailedExportControlNotAllow alarm has been added. For more details on this alarm, see the Cisco Unified Serviceability interface.

Alert

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

- SmartLicenseAuthorizationExpiringSoon
- SmartLicenseCommunicationError
- SmartLicenseExportControlNotAllowed
- SmartLicenseInEval
- SmartLicenseInOverageAuthorizationExpired
- SmartLicenseInOverageOutOfCompliance
- SmartLicenseNoProvisionAuthorizationExpired
- SmartLicenseNoProvisionEvalExpired
- SmartLicenseNoProvisionOutOfCompliance
- SmartLicenseRegistrationExpired
- SmartLicenseRegistrationExpiringSoon

- SmartLicenseRenewAuthFailed
- SmartLicenseRenewRegistrationFailed

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

Upgrade and Migration Updates

The upgrade and migration details to support this feature is detailed below.

Migration of PLM Licenses to Smart Entitlement

If you are eligible to upgrade to the Smart Licensing version of the product, then you are able to initiate the migration through the License Registration Portal or Cisco Smart Software Manager. You can self-initiate this process by downloading and installing the Smart Licensing version of the software and registering the device to a Smart Account using a Registration Token. The migration of any entitlements tracked by Cisco automatically migrates to the Customers Smart Account. You will also be able to initiate the migration of unused classic PAKs to Smart Accounts for future consumption by products in Smart Mode. This process is available through the License Registration Portal or Cisco Smart Software Manager.

Unified Communications Manager 9.0x and later version of 12.0(1)

- If you are holding an active Cisco Software Support Service (SWSS) contract, then you can convert the classic licenses to smart entitlements through the Cisco Smart Software Manager at https://software.cisco.com/#SmartLicensing-LicenseConversion.
- Two types of Migration are supported:
  - PAK based—Supported for already fulfilled, partially fulfilled and unfilled PAKs
  - Device based
- Partial Conversion supports mixed environment of older and Unified Communications Manager 12.0(1) clusters.

Upgrade to Smart Entitlement

Unified Communications Manager Pre 9.0x (Device based) to 12.0(1)

You may contact Cisco Global Licensing Operations (GLO) for helping with migrating Device-based licenses to Smart Entitlement.

Customer may establish equivalent user-based licensing required by running License Count Utility (LCU). For more details, see http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/upgrade/uct/CUCM_BK_UCT_Admin_Guide/CUCM_BK_UCT_Admin_Guide_chapter_01.html.

From the LCU report, Customer may order respective quantity of Upgrade Licenses through Cisco Commerce Workspace. Beyond this, they would have to buy additional new licenses. For more details, see the Ordering Guide at http://www.cisco.com/c/en/us/partners/tools/collaboration-ordering-guides.html.

CTL Updates

To enable the mixed mode or to update the CTL File, ensure that the Smart Licensing registration is completed in Cisco Unified Communication Manager by using the Registration Token received from the Smart account or Virtual account that has Allow export-controlled functionality enabled.

If you have enabled the mixed-mode prior to upgrade and have not registered to Cisco Smart Software Manager or Cisco Smart Software Manager satellite then:

- You see the warning message in the Cisco Unified CM Administration page and Cisco Unified OS Administration page as stated below:

Warning The system is currently running Mixed mode. To continue running Mixed mode, please ensure Smart Licensing registration is completed using the Registration Token received from the Smart/Virtual Account that has Allow export-controlled functionality checked.

- An alert named *SmartLicenseExportControlNotAllowed* is sent, when the Cisco Unified Communications Manager is not registered with the Registration Token.

Supported LDAP Directories

For this release of Cisco Unified Communications Manager, following is the full list of supported LDAP directories:

- Microsoft Active Directory 2008 R1/R2
- Microsoft Active Directory 2012 R1/R2
- Microsoft Lightweight Directory Services 2008 R1/R2
- Microsoft Lightweight Directory Services 2012 R1/R2
- Microsoft Active Directory 2016
- Oracle Directory Server Enterprise Edition 11gR1
- Oracle Unified Directory 11gR2
- Open LDAP 2.4.44 or later

Voicemail Launch from Self Care Portal

For this release, the Unified Communications Self-Care Portal has been enhanced with an option to launch a user's Cisco Unity Connection Web inbox from within the Self-Care Portal. From within the Self-Care Portal, users can select the **Voicemail** tab and then click the **Launch Voicemail Inbox** button. A new tab will open at the Cisco Personal Communications Assistant login screen.

Prerequisites

Before end users can use this feature, administrators must configure the following in Cisco Unified Communications Manager:

- Configure the user with a Service Profile that includes a voicemail service and a mailstore service (if visual voicemail is used). For details, see the "Configure Service Profile" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*.
- Configure Cisco Unity Connection integration. For details, see the "Configure Cisco Unity Connection for Voicemail and Messaging" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*.

Launch Voicemail Inbox

To launch your voicemail inbox, complete these steps:

Procedure

Step 1 In the Self-Care Portal, select the **Voicemail** tab.

Step 2 Click the **Launch Voicemail Inbox** button.
The portal launches the Cisco Personal Communications Assistant web application.

Web Browser Security Enhancement

After a system logoff, Cisco Unified Communications Manager does not allow an administrator to use the web browser's **Back** button to return to the Cisco Unified Communications Manager interface without logging in. This security enhancement provides additional data security and confidentiality by preventing unauthenticated access to the Cisco Unified Communications Manager interface.

Web Browser Support

This feature offers web browser support for seamless access to each of the Cisco Unified Communications Manager web application. Examples of such applications are Cisco Unified CM Administration, Cisco Unified Serviceability, and Cisco Unified Operating System Administration. Beginning from Release 12.0, the following web browsers are supported:

- Firefox with Windows 10 (64 bit)—Latest browser version only
- Chrome with Windows 10 (64 bit)—Latest browser version only
- Internet Explorer 11 with Windows 10 (64 bit)
- Internet Explorer 11 with Windows 8.1 (64 bit)
- Internet Explorer 11 with Windows 7 (64 bit)
- Microsoft Edge browser with Windows 10 (32 bit/64 bit)

- Safari with MacOS (10.x)—Latest browser version only