New and Changed Features

Additional Billing Server Support

You can now add up to eight billing servers in Unified Communications Manager.

AV1 Codec Support

Unified Communications Manager now supports negotiation and passthrough of AVI codec. The AV1 is a modern codec that provides better compression and hence can provide the same user experience as H.264 video codec at half the bandwidth. AV1 codec will be supported by Cisco Webex Desk Pro Endpoint, Webex Codec Pro, and Room Panorama systems.

See the compatibility matrix for the compatible version of Webex Room devices, Cisco Expressway, and Cisco Meeting Server.

Cisco Tomcat Containerization

Releases prior to 14 have single instance of Cisco Tomcat managing many web applications with limited resource control and throttling. When resource-intensive applications like UDS, AXL, and SSOSP run along with other web applications, it makes the user interface sluggish. Also, this impacts the Cisco Tomcat memory management and results in higher CPU consumption.

The Cisco Tomcat service within the Unified CM virtual machine is now containerized. The benefits of containerization include:

- Enhance application stability
- Faster startup time
- Rate-limiting at an individual application level
- Improved serviceability to monitor web sessions per application

Web applications such as AXL, UDS, and SSOSP are now containerized with their own Tomcat instance running inside each container while all other web applications are running on the Cisco Tomcat instance. Following are the new Tomcat services introduced and running within the containers:

- Cisco AXL Tomcat
- Cisco UDS Tomcat
- Cisco SSOSP Tomcat

The other Unified Communications Manager web applications continue to run outside the containers on the existing Cisco Tomcat.

Managing Containers for Unified CM

Command Line Interfaces (CLI) Introduced for Cisco Tomcat Containerization

The following new commands are introduced to support this feature:

- **utils container-engine start**
- **utils container-engine stop**
- **utils container-engine restart**
- **utils container-engine status**

- **utils diagnose test**
- **utils diagnose module <module_name> <container_name>**

You can start, stop, or restart operation on individual tomcat containers by using the following CLI command: **utils service restart/stop/start <tomcat_service_name>**.

To obtain the tomcat service name to be used in this command, run the **utils service list** CLI command that will display the following new tomcat services introduced as part of this feature.

- Cisco AXL Tomcat (for AXL container restart)
- Cisco UDS Tomcat (for UDS, CCMPD, and CCMCIP container restart)
- Cisco SSOSP Tomcat (for SSOSP container restart)

Use the following commands to collect logs:

- **file get activelog tomcat/logs/axl-tomcat/***
- **file get activelog tomcat/logs/uds-tomcat/***
- **file get activelog tomcat/logs/ssosp-tomcat/***

For more information on the services, see the *Cisco Unified Serviceability Online Help*.

For more details about the CLI commands, see the "Utils Commands" chapter in the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

Monitoring Containerized Tomcat Web Applications Status

You can monitor containerized Cisco Tomcat web applications using the Unified Real-Time Monitoring Tool (RTMT) user interface.

Performance counters are added in the RTMT to monitor the newly added services: Cisco AXL Tomcat, Cisco UDS Tomcat, and Cisco SSOSP Tomcat.

- Docker Container
- Cisco AXL Tomcat Connector
- Cisco AXL Tomcat JVM
- Cisco AXL Tomcat Web Application
- Cisco UDS Tomcat Connector
- Cisco UDS Tomcat JVM
- Cisco UDS Tomcat Web Application
- Cisco SSOSP Tomcat Connector
- Cisco SSOSP Tomcat JVM
- Cisco SSOSP Tomcat Web Application

For more information, see the System Counters section in the ‘Performance Counters and Alerts’ chapter in the Cisco Unified Real-Time Monitoring Tool Administration Guide, Release 14.

Troubleshoot Cisco Tomcat Containers

1. **Problem Symptoms**: Multiple users experience login failures using Cisco Jabber or Webex App.

   Solution:

   a. Navigate to **Cisco Unified Serviceability > Tools > Control Center - Network Services**. Check the following tomcat services: Cisco UDS Tomcat and Cisco SSOSP Tomcat.

   b. (OR) Run the **utils container-engine status** command using CLI.

   c. If any of these tomcat services is not running, restart the Cisco UDS Tomcat or Cisco SSOSP Tomcat service that is causing the error using the **utils service restart<tomcat_service_name>** CLI.

   d. If the issue still persists, contact Cisco Technical Assistance Center (TAC).

2. **Problem Symptoms**: AXL/UDS applications experiences slowness.

   Solution:

   a. From Cisco Unified Real-Time Monitoring Tool, navigate to **Performance**, select the standalone cluster, and open the node where the AXL/UDS application is connected. Monitor the following counters under the Cisco AXL Tomcat Connector/Cisco UDS Tomcat Connector or Cisco AXL Tomcat Web Application/Cisco UDS Tomcat Web Application performance counters:

      1. Errors
      2. Requests
      3. ThreadsBusy
      4. SessionsActive

   b. Apart from these counters, if any other counter values are not decremented and the application is still utilizing high CPU, contact Cisco Technical Assistance Center (TAC).

3. **Problem Symptoms**: AXL becomes unresponsive.

   Solution:

   a. Navigate to **Cisco Unified Serviceability > Tools > Control Center - Network Services**. Check the Cisco AXL Tomcat service.

   b. (OR) Run the **utils container-engine status** command using CLI.

   c. If the Cisco AXL Tomcat service is not running, restart the Cisco AXL Tomcat service that is causing the error using the **utils service restart<tomcat_service_name>** CLI.

   d. If the issue still persists, contact Cisco Technical Assistance Center (TAC).

4. **Problem Symptoms**: Application user interfaces experience slowness/inaccessible.

   Solution:

   a. From Cisco Unified Real-Time Monitoring Tool, navigate to **Performance**, select the standalone cluster, and open the node where the application is connected. Monitor the following counters under the Cisco Tomcat Connector or Cisco Tomcat Web Application:

      1. Errors

2. Requests
3. ThreadsBusy
4. SessionsActive

b. If the application user interface is inaccessible, run the command utils service list and check the Cisco HAProxy and Cisco Tomcat services status. If these services are down, restart the Cisco HAProxy and Cisco Tomcat services.

c. If the issue still persists, contact Cisco Technical Assistance Center (TAC).

Certificate Regeneration without Service Restarts

A manual restart of the CallManager and CTIManager services are no longer required when a CallManager certificate is regenerated on Unified Communications Manager. A new enterprise parameter **Phone Interaction on Certificate Update** under section **Security Parameter** is introduced to reset phones either manually or automatically as applicable, when one of TVS, CAPF or TFTP certificates are updated for this release in Unified Communications Manager. This parameter is by default set to reset the phones automatically.

You don’t have to restart the CallManager service when OAuth is enabled and the Tomcat certificate is regenerated. CAPF service is auto restarted when the CAPF certificate is regenerated or any new certificate is uploaded to CAPF trust.

For more information on Certificate Regeneration without Service Restarts, see the "Certificate Management" chapter in the Security Guide for Cisco Unified Communications Manager.

Fresh Install with Data Import

Virtual to Virtual (V2V) migration make it easy to upgrade and migrate Unified Communications Manager. In the same process, you can upgrade the Unified Communications Manager version, move to a new virtual machine configuration, migrate data between clusters, upgrade the VMware vSphere ESXi version, and migrate to new hardware if desired.

Fresh Install with Import Data also provides an alternative to Direct Refresh Upgrade and PCD Migration (for scenarios where temporary migration hardware or configuration of management applications is undesirable).

You can:

- Export data from an existing cluster to an SFTP server.
- Perform fresh installation of a new cluster and import data from the SFTP server into the new cluster. This can be done through the touchless installation as well. An option for data import appears in new sections of the install wizard and Answer File Generator.

For more information on Install with Data Import, see the Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service.

CLI Update

To support data export from your old system to the SFTP server, use the following commands:

- **utils system upgrade dataexport initiate**
- **utils system upgrade dataexport status**
- **utils system upgrade dataexport cancel**

For more details about the CLI commands, see the "Utils Commands” chapter in the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

Enable SIP OAuth for 78xx and 88xx Phones

SIP OAuth provides end to end secure signaling and media encryption without CAPF on-premises as well as over MRA and by default, TFTP is secure for SIP phones when SIP OAuth is enabled.

For more information on the following, see the System Configuration Guide for Cisco Unified Communications Manager:

- Configuring Cisco IP Phones, see chapter "Configure Cisco IP Phones".
- Configuring Activation Code Onboarding, see chapter "Device Onboarding via Activation Codes".

Enhanced Accessibility and Usability in Self Care Portal

The Self Care Portal is enhanced with the following accessibility improvements for the phone features and settings:

- Font type and size—Consistent usage of the Sans-serif font type with a minimum of 10 dpx size across the Self Care Portal.
- Keyboard navigation—Better navigation support for pages under **Phones>My Phones** Menu Item.
- Screen reader and compatibility—Ease of viewing content and navigation for screen reader users.

Enhanced Security Compliances

As part of Cisco's continuous review of the Unified Communications Manager and IM and Presence Service architecture to identify security vulnerabilities and weaknesses, the following compliance and validation investments were made as part of the security compliances roll-out:

- Cross-Site Scripting Vulnerability—A vulnerability in the web-based management interface of Unified Communications Manager and IM and Presence Service is addressed so that it does not allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. Open Web Application Security Project (OWASP) encoding guidelines were implemented to fix the XSS vulnerabilities.
- Standard Practices Followed for X.509 Certificate Validation—Ensure the name or identification information (FQDN) that is presented in the certificate Subject Name of the peer being authenticated matches with the peer the Unified Communications Manager is communicating with. Always reject expired or invalid certificates. Users should also ensure that there is only one X.509 extension of any type in the certificate list before accepting the certificates you receive from the web server.

- Certificate Validity—Addresses the Lifetime of Certificates to achieve security compliance.
  - TLS-based (server) Certificates have a lifetime of three years.
  - Signing Certificates are by default restricted to a lifetime of five years.
  - ITLRecovery Certificates have a lifetime of 20 years.

  ITLRecovery file signs the ITL and CTL files and any change in these certificate validities affect the trust model with phones.

  For more information on Certificate Validity, see the chapter "Certificate Management" in the *Security Guide for Cisco Unified Communications Manager*.

- Digitally Sign Software and Control Keys—Post Release 14, the SHA512SUM hash-based signing tool improves security to upgrade all COP and ISO files.

  All new COP and ISO files now have a '.sha512' extension in their names instead of the '.sgn' extension. For example: ciscocm.free_common_space_v1.5.cop.sha512.

  For more information, see the *Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service*.

Granular Access Control Enhancements

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

User Interface Updates

The following fields are introduced:

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

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

Headset and Accessories Inventory Download

The **Headsets** menu category is renamed to **Headsets and Accessories** in the Cisco Unified Communications Manager user interface.

This feature enables an administrator to download a detailed report of Headsets and Accessories in your deployment into a CSV file from the Unified Communications Manager user interface.

For more information, see the “Headset and Accessories Management” chapter in the Feature Configuration Guide for Cisco Unified Communications Manager.

SAML Based Single Logout

The Unified Communications Manager now includes a new feature to support SAML based Single Logout (SLO).

SAML based Single Logout allows you to logout simultaneously from all sessions of a browser that you have signed in using SAML based Single Sign-On (SSO).

For more information, see the "SAML-Based SLO" chapter in the SAML SSO Deployment Guide for Cisco Unified Communications Applications.

MRA Failover with Lightweight Keepalives

The MRA High-Availability for endpoint registration feature allows Cisco Webex and Cisco Jabber clients to quickly detect any failure of network elements like Cisco Expressway-E, Cisco Expressway-C, or Unified Communications Manager in the path and take corrective action to re-register using a new path. It sends a lightweight STUN keepalive message to reregister to the Unified CM through the next available path.

When the Unified Communications Manager receives the lightweight STUN keepalive message, it validates Cisco Expressway-C IP and responds to the message.

For more information, see the 'MRA Failover with Lightweight Keepalives' section in the "Configure Mobile and Remote Access" chapter of the Feature Configuration Guide for Cisco Unified Communications Manager. And check the *Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service* to get information about compatible versions of Cisco Webex, Cisco Jabber, and Cisco Expressway.

Native Phone Migration using IVR and Phone Services

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

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

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

Table 1: Different Phone Migration Options and Considerations

	Using Self-provisioning IVR Service	Using Phone Migration Service	Using Unified CM Administration Interface
End user or administrator driven phone migration	End user (Self-service)	End user (Self-service)	Administrator

	Using Self-provisioning IVR Service	Using Phone Migration Service	Using Unified CM Administration Interface
Auto-registration required	Yes	No	No
Migration steps	• Auto register a new phone • Dial self-provisioning IVR number • Follow the voice prompts	• Plug-in new phone to the network • Key in primary extension and PIN (optional)	• Sign in to Cisco Unified CM Administration interface • Choose "Migrate Phone" option in the Phone Configuration page of the old phone • Enter phone type (model & protocol) and MAC address of the new phone
Administrator involvement	Medium	Low	High

For more information, see the "Native Phone Migration using IVR and Phone Services" chapter in the Feature Configuration Guide for Cisco Unified Communications Manager.

User Interface Updates

The following fields are added:

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

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

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.

Phones with Mismatched ITL Checksums

When Call Manager Certificate is renewed, the phones reset and obtain new ITL files. During this process, some phones may retain the old ITL files. The Unified Communications Manager now allows the administrator to identify SIP phones that have older ITL files and provides the centralized report of phones with mismatched ITL files.

User Interface Updates:

In **Device** > **Phone** > **Find and List Phone** page, a new drop-down list **ITL File Status** is added:

- Match
- Mismatch
- Not Installed
- Unknown

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

Simplified Certificate Management

Unified Communications Manager and the IM and Presence Service now includes a new feature to reduce the number of Identity Certificates.

The certificates should be renewed periodically based on their validity period and it is difficult to manage these certificates in a multi-cluster deployment scenario.

You now have an option to efficiently reduce and reuse the number of certificates. With fewer certificates to monitor, the job of an administrator to monitor, renew and update certificates is simplified.

For more information, see the "Certificate Management and Simplification" chapter in the Security Guide for Cisco Unified Communications Manager.

UDS Enhancements

The following enhancements are introduced for UDS:

- The UDS Bulk Search by Email enables Cisco Jabber to send requests in batches using the email attribute to prevent high CPU usage by UDS and Cisco Tomcat services.
- UDS is enhanced to do a better discovery of the home cluster of a user across remote clusters. This helps in avoiding the Cisco Jabber login failures and ensures geo redundancy in the event of Data Center failure or shutdown.

Version Independent Licensing

Unified Communications Manager supports Version Independent User Licenses. The Licenses are annuity-style and issued for the subscription term. You can order these V14 licenses through Flex EA (Enterprise Agreement) or Flex NU (Named User—Professional, Enhanced, Access). For more information, see the Ordering Guide.

Unified Communications Manager 12.x continues to use the version 12.X License.

The licenses are managed on CSSM (Cisco Smart Software Manager). For more information, see the "Smart Software Licensing" chapter in the System Configuration Guide for Cisco Unified Communications Manager.

Wi-Fi to LTE Call Handoff

Wi-Fi to LTE Call Handoff provides flexibility for Cisco Webex users to switch between Wi-Fi and LTE networks without disconnecting any active calls that the user may be while switching network.

This feature is supported on both Cisco Webex Mobile and Desktop versions.

For more information, see the 'Wi-Fi to LTE Call Handoff' section in the Feature Configuration Guide for Cisco Unified Communications Manager.

Windows 2019 Support for RTMT

You can install Cisco Unified Real-Time Monitoring Tool on a computer that is running on Windows 2019 operating system to monitor or troubleshoot Unified Communications Manager.

Certificate Sync and Intercluster Periodic Sync

The IM and Presence Service performs certificates sync as part of the intercluster sync process. This feature introduces a new service parameter **Certificate Sync during Inter-Cluster Periodic Sync** and allows the administrator to disable or enable certificates synchronization as part of Intercluster periodic sync from the Cisco Unified Communications Manager IM and Presence Administration user interface.

The Certificate Sync feature intoduces the following options:

- **Perform certificate sync**—This is the default value of the **Certificate Sync during Inter-Cluster Periodic Sync** service parameter. When the **Certificate Sync during Inter-Cluster Periodic Sync** service parameter is set to **Perform certificate sync** and the certificates are not synchronized across the intercluster peers, it requires a Force Manual Sync operation to synchronize data and certificates.

- **Do not perform certificate sync**—To disable the certificate sync during the ICSA sync, the administrator can set the **Certificate Sync during Inter-Cluster Periodic Sync** service parameter to **Do not perform certificate sync**.

Note If you encounter performance degradation or high CPU spikes in your deployment that is related to certificate sync during intercluster periodic sync, you can use this feature.

For detailed information on how to disable or enable certificates sync as part of the intercluster sync process, see the "Configure Intercluster Peers" chapter in the Configuration and Administration of the IM and Presence Service Guide.

Deletion of Intercluster Peers does not Require XCP Router Restart

The IM and Presence Service is enhanced to prevent restart of XCP router on each node within the IM and Presence cluster after deleting an intercluster peer. This enhancement helps the administrator manage large-scale clusters effectively by significantly reducing the overhead caused by sequential restart of nodes while ensuring uninterrupted Cisco Jabber service.

For more information, see the 'Delete Intercluster Peer Connections' section of the "Configure the System" chapter in the Configuration and Administration of the IM and Presence Service Guide.

IM and Presence Configuration for SIP Open Federation

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

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

IM and Presence Failover Enhancement to Nearly Zero Downtime

IM and Presence Service is enhanced to reduce the impact during upgrade and failover of nodes and clusters, and hence minimize the Jabber service outage.

In Release 14, IM and Presence Service supports dual connection with Jabber clients. When enabled on the client side, this type of connection ensures much shorter (nearly zero) service downtime during High Availability failover events.

It helps to:

- Minimize service disruption to Jabber clients during direct standard upgrade of IM and Presence Service.
- Provide seamless transition of the user session between the primary and the secondary node.

For more information, see the 'IM and Presence Failover Enhancement to Nearly Zero Downtime' section of the "Configure Centralized Deployment" chapter in the Configuration and Administration of the IM and Presence Service Guide.

For version compatibility for all Cisco Jabber clients, see the Compatibility Matrix for Cisco Unified Communications Manager and IM & Presence Service.

Improved IM and Presence Stream Features/Services Advertisement via Expressway

IM and Presence Service now supports the advertisement of XMPP stream features/services to the clients connecting over Cisco Expressway's Mobile and Remote Access.

This new functionality enables deployments with mixed IM and Presence Service versions, for example some clusters on 11.5(1)SU8 and some other clusters on 12.5(1)SU3, to work with Cisco Expressway so that Cisco Jabber clients can discover the correct capabilities applicable to it based on the IM and Presence Service home cluster it is assigned to.

For this mechanism to work, the minimum deployment requirement is to have Cisco Expressway running version X12.7 or higher and have at least one IM and Presence cluster in the intercluster mesh running version 11.5(1)SU9 or 12.5(1)SU4 and above.

Depending on your current IM and Presence Service version mix, you may need to enable or disable push notifications feature using FCM service flag on the Expressway as per the information given in the following table:

```
xConfiguration XCP Config FcmService: On/Off
```

Note Apple Push Notification Service (APNS) is not affected by the FCM service flag status.

Table 2: Solution Matrix from the Perspective of Expressway CLI Enable/Disable Command for Android Push Notifications (FCM)

Mixed Versions IM and Presence Clusters	Expected Status of FCM Flag on Expressway X12.7	Comment
Any 11.5(1)SU with 12.5(1)SU2 and lower	OFF	Android Push (FCM) NOT supported.
11.5(1)SU8 (and lower) or 12.5(1)SU2 (and lower) with 12.5(1)SU3	OFF	Android push (FCM) NOT supported
11.5(1)SU8 (and lower) or 12.5(1)SU2 (and lower) with 12.5(1)SU4 (and higher)	OFF	Android push (FCM) supported on 12.5(1)SU4 (or newer) versions
11.5(1)SU9 (and higher) or 12.5(1)SU4 (and higher) with 12.5(1)SU3	ON	Android push (FCM) supported on version 12.5(1)SU3 and higher
11.5(1)SU9 (and higher) with 12.5(1)SU4 (and higher)	Flag not required (Expressway 12.7 relies fully on the new discovery mechanism)	Android push (FCM) supported on 12.5(1)SU4 (or newer) versions

Jabber User Location Migration

The IM and Presence Service supports the migration of locations that are configured by Jabber users, from one IM and Presence Service cluster to another. The user location migration feature is implemented as an extension to the existing Bulk Administration feature available under the Cisco Unified Communications Manager IM and Presence Administration user interface.

The administrator can export all user locations configured on a Source IM and Presence Service cluster to a CSV file and import the exported CSV file by uploading it on the Destination IM and Presence Service cluster. You can perform this by triggering the **User Location Import** option which reads the data from the uploaded CSV file and inserts these records into the IM and Presence Service database.

For more information, see the 'Bulk Administration of Contact Lists' section of the "Administer the System" chapter in the Configuration and Administration of the IM and Presence Service Guide.

Out of Office Presence Status

The IM and Presence Service supports Out of Office (OOO) as the user’s availability status. As a result, when you set the out of office notification in Miscrosoft Outlook for a specific duration, your Jabber presence status displays as **Out of Office** instead of showing **Away** or **Offline**. Moreover, this feature improves the user experience of the instant messaging system by allowing other users know your availability as Out of Office along with the start and end dates.

For more information, see the “Office 365 Out of Office Notification Presence State” chapter in the Microsoft Outlook Calendar Integration for the IM and Presence Service.

Push Notification Support for Jabber MAM Clients

The IM and Presence Service extends its Push Notification feature support for Mobile Application Management (MAM) clients like Cisco Jabber for Intune and Cisco Jabber for BlackBerry. As a result, the push notification service is available for all devices that are running Cisco Jabber for Intune and Cisco Jabber for BlackBerry clients.

For more information on how to deploy push notification, see the Push Notification Deployment Guide.

User Session Report for Device Capacity Monitoring

The Device Capacity Monitoring feature lets IM and Presence Service administrators view the User Session Report of the active users logged in from multiple devices. This report can be viewed at the cluster, sub cluster, and node level.

Cluster level reports display the following fields:

- Presence Redundancy Group
- Node Name
- Count of users logged in from one or more devices
- Total number of sessions at the cluster, sub cluster, and node level along with the date and timestamp of the report generated

Based on the count of users logged in from one or more devices, you can generate the detailed user-based report for a particular node. From the Reports window, you can download reports to a CSV file.

To generate the reports, log in to **Cisco Unified IM and Presence Reporting** and choose **System Reports** > **IM and Presence User Sessions Report**.

For more information, see the 'User Session Report for Device Capacity Monitoring' section of the Configuration and Administration of the IM and Presence Service Guide.