# New and Changed Features


- Calendar Integration with Office 365 Support for OAuth 2.0 authentication, on page 1
- Certificate Revocation with Online Certificate Status Protocol, on page 2
- Phone Replacement and Migration Using Self-Provisioning, on page 2
- Presentation Setting on Caller's Directory Number, on page 3
- Self Provisioning of Analog Phones, on page 3
- Support for LDAP Credentials in Cisco Jabber Service Profile, on page 3
- User Session Report for Device Capacity Monitoring, on page 4
- Migrate Persistent Chat Rooms from One External Database to Another, on page 4


## Calendar Integration with Office 365 Support for OAuth 2.0 authentication

The IM and Presence Service's Calendar Integration with Office 365 feature is enhanced to support the usage of OAuth tokens for authenticating to the Office 365 server. This enhancement allows a more streamlined and secured authentication process than the regular password-based authentication.

When you configure Calendar Integration with an Office 365 server, the IM and Presence Service lets you choose from two authentication options:

- **Basic**—password-based logins
- **OAuth**—authentication with OAuth tokens

**Note** Basic authentication method will be supported as long as Microsoft supports it. When Microsoft deprecates, it will be deprecated from IM and Presence Service.

If you choose OAuth, you must configure the following fields, each of which are added to the Presence Gateway Configuration window for this release. These fields are included for OAuth logins only:

- Application (client) ID
- Directory (tenant) ID
- Client Secret

For more information on how to configure the IM and Presence Service for Calendar Integration with an Office 365 server, see the Microsoft Outlook Calendar Integration for the IM and Presence Service.

# Certificate Revocation with Online Certificate Status Protocol

Certificate Revocation with Online Certificate Status Protocol (OCSP) improves the security of your system.

Both FIPS and non-FIPS deployments can use OCSP to check the certificate validity and revocation status for CA-signed certificates. The validation ensures that your system doesn't make TLS connections to entities with revoked certificates.

OCSP works only for CA-signed certificates and not for self-signed certificates.

Enable the OCSP for the certificate to return a Good, Revoked, or Unknown status once the configured OCSP Responder validates the certificates.

Common Criteria deployments only accept certificates with a Good status. Non-FIPS deployments accept certificates with a Good or Unknown status and reject certificates with a Revoked status.

Enable OCSP and assign an OCSP URI in the Certificate Revocation window of the Cisco Unified OS Administration to use the functionality.

For more information on OCSP, see the "Certificate Revocation" chapter of the Security Guide for Cisco Unified Communications Manager.

# Phone Replacement and Migration Using Self-Provisioning

Use the Self-Provisioning IVR service in Unified Communications Manager to directly migrate or replace a faulty desk phone or lobby phone without the need to contact the administrator. This feature makes it simple to replace phones while minimizing costs at the same time.

Migration using Self-Provisioning in Unified Communications Manager minimizes the initial configuration requirement while migrating the existing phone settings to the new phone. You can choose to delete or retain the old phones in Unified Communications Manager when provisioning a phone for migration or replacement.

For more information, see the "Phone Replacement and Migration Using Self-Provisioning" chapter of the Feature Configuration Guide for Cisco Unified Communications Manager.

### User Interface Updates

To support this feature, the following sections 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.
- 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 more information, see the *Cisco Unified Administration CM Administration Online Help*.

# Presentation Setting on Caller's Directory Number

Unified Communications Manager honors the caller's calling line identity setting when a call is forwarded to a PSTN number when the Presentation Setting on caller's directory number feature is enabled. The presentation setting takes precedence over forwarding patterns and other settings that modify the caller's presentation setting, such as translation patterns, route patterns, and trunk settings.

### User Interface Updates

To support this feature, the following fields are added:

- In the **Directory Number Configuration** window, the **Calling ID Presentation When Diverted** field is added.

  For more information, see the **Call Routing Menu** > **About Directory Number Setup** > **Directory Number Settings** section in the *Cisco Unified Administration CM Administration Online Help*.

- In the **Trunk Configuration** window, the **Use original calling line's Calling Line ID Presentation for diverted calls** check box is added.

  For more information, see the **Device Menu** > **About Trunk Setup** > **SIP Trunk Settings** section in the *Cisco Unified Administration CM Administration Online Help*.

# Self Provisioning of Analog Phones

You can enable self-provisioning on auto-registered analog FXS ports so that the users can call the self-provisioning IVR and assign their associated directory number to that analog port. This feature makes it simple for users to assign phones or replace faulty phones without help from administrator.

The auto-registration feature now supports analog phones over VG400, VG450, and ISR4K series IOS-XE voice gateways using SCCP protocol (IOS-XE 17.1+).

For more information, see the "Enable Auto Registration for Analog Phones" and "Self Provisioning Analog FXS Ports" sections in System Configuration Guide for Cisco Unified Communications Manager.

# Support for LDAP Credentials in Cisco Jabber Service Profile

The Directory Profile in the Service Profile Configuration window of Unified Communications Manager is enhanced to support secure LDAP credentials (username and password) for encrypted Cisco Directory integration (CDI). This update secures access to your directory by ensuring that the password is always stored and sent in an encrypted format. This includes encryption during directory access authentication, client configuration file downloads, BAT imports/exports, and upgrades.

Prior to Release 12.0, Unified Communications Manager supported LDAP credentials for authentication. However, this support was removed in the subsequent releases due to security issues that allowed the directory

password to be compromised during upgrades or BAT import and export operations. This update introduces the feature, while also addressing the previous security issues.

**Note** If you are using the LDAP credentials for authentication, you should disable the **Cisco Jabber Diagnostic Tool** using the **DiagnosticsToolEnabled** parameter configured in the Jabber Client Configuration (jabber-config.xml) file.

For more information, see the "Import Configuration to Server" section in the Bulk Administration Guide for Cisco Unified Communications Manager.

# 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.

# Migrate Persistent Chat Rooms from One External Database to Another

IM and Presence Service allows customers to migrate all persistent chat rooms and user groups across multiple external databases of the same type or different types. This feature provides additional controls in managing your external database environment by letting you move persistent chat rooms between external databases within the same IM and Presence node. For example, it enables you to move all the persistent chat rooms from one external database to another, such as from Oracle to Oracle, Oracle to PostgreSQL, and MSSQL to Oracle.

For more information on how to perform the external database migration, see the "Migrate Persistent Chat Rooms from One External Database to Another" section of the Database Setup Guide for the IM and Presence Service.