New and Changed Features

MRA Device Onboarding using Activation Codes

This release extends the on-premise Activation Code Device Onboarding feature to also work for Mobile and Remote Access endpoints that are connecting remotely. This update provides a secure way to onboard MRA endpoints that are onboarding remotely. It also simplifies the user experience by removing the requirement that MRA users be within the enterprise network when they onboard their endpoints for the first time.

When remote MRA users connect their phone for the first time, the phone communicates with the Cloud/Hybrid Service in order to obtain the activation code requirement. The MRA users can pick up the activation code from the Self-Care Portal and then enter the code on the phone in order to complete the initial registration. This process works even if the phone cannot reach the cluster TFTP server.

As a part of this feature, OAuth Refresh Logins are introduced for Cisco IP Phones that are onboarded over MRA using device activation codes.

Configuration

For more information, see the "Device Onboarding via Activation Codes" section of the *System Configuration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU1*.

Phone Support

This feature is supported for the following Cisco IP Phones:

7811, 7821, 7832, 7841, 7861, 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NR, 8832, 8832NR

User Interface Updates

The following configuration windows are added or updated:

- **Cisco Cloud Onboarding**—This page is updated with a new section, **Activation Code Onboarding Settings** that contains the following fields:
  - Enable Activation Code Onboarding with Cisco Cloud
  - MRA Activation Domain
  - Trusted CA Certificates--Used by devices to secure communication with your Expressway(s)' is added.
  - This page is also updated with helpful status information for viewing the status of activation code registrations for MRA endpoints.
- **MRA Service Domain Configuration**—This new page is added to the **Advanced Features** menu. The page lets you enter the SRV record and device pool for an MRA Service Domain. It contains the following fields:
  - Name
  - Domain
  - Default
  - Dependency Records
- **Device Pool Configuration**—A new **MRA Service Domain** drop-down is added.
- **Device Defaults**—The Onboarding method column is renamed to **On-Premise Onboarding Method.** This field applies to on-premise onboarding only and does not apply to onboarding for MRA devices using activation codes.
- **Phone Configuration**—The new **Allow Activation Code Onboarding via MRA** check box is added.
- **Enterprise Parameters Configuration**—A new parameter, **Physical Phone OAuth Refresh Token Expiry Timer**, is added with a default value of 60 days.

Serviceability Updates

The following new alarms are added for activation code onboarding:

- **DevActAccessTokenInvalid**—The access token used by the Cisco Device Activation Service to communicate with the Cisco Cloud was not able to be renewed and has expired.
- **DevActCloudSyncFailure**—An automatic attempt to synchronize configuration changes with Cisco Cloud related to Device Activation Coe-based onboarding has failed.

- **Dev ActSSOSPServerRemoved**—An SSOSP service is not responding properly during an activation code device onboarding event and has been removed from the list of servers leveraged to provide refresh tokens to the onboarding phone.

Certificate Updates

A new certificate trust store (**PhoneEdge-trust**) is added to Cisco Unified OS Administration. If you want to use your own certificates, you can upload your own custom certificates that MRA endpoints will use to connect to Expressway.

The certificate must first be uploaded to the Expressway servers and then uploaded to this new trust store on Cisco Unified Communications Manager, following which the certificate gets transmitted to the cloud. When the phone is onboarded over MRA using activation codes, the phone downloads the certificate from the cloud and uses it to establish trust with Expressway.

Change in SHA-1 or MD5 Algorithm Values

This feature improves security when onboarding new phones. With this update, the SHA-1 and MD5 algorithms in the Initial Trust List (ITL) file remain unchanged unless there is a change in the ITL file. You can compare the checksum value of the phone's ITL file against the checksum value in Unified Communications Manager as a check to verify the onboarding process and the trust state of the phones.

For more information, see the “Initial Trust List” section, of the *Security Guide for Cisco Unified Communications Manager.*

CTI Monitoring

In this release, the Unified Communication Manager enables CTI monitoring for Cisco dual-mode devices such as for Android, iPhone, and iPad. These devices are monitored and not controlled through CTI.

For a CTI application user, the interface of CTI provides information about the controlled Cisco dual-mode devices so that they identify the devices that are available for monitoring and controlling. CTI Application user can monitor the devices in WiFi mode that are available in the control list to track the device status (idle or busy).

User Interface Updates

To enable this feature, check the **Allow Control of Device from CTI** check box in the **Device** > **Phone** > **Phone Configuration** window.

For more information, see "Phone Settings" section field description in the *Cisco Unified Administration CM Administration Online Help*.

Device Capacity Monitoring

The IM and Presence Service is updated with new counters to help you monitor Jabber client registrations and keep your system up and running.

This feature addresses performance issues that can result when you have Multiple Device Messaging (MDM) deployed and the number of client registrations gets out of hand. With MDM, each client registration counts as a separate user. If a single user has multiple Cisco Jabber client registrations (for example, one registration on a laptop, and one on a mobile phone), each registration counts as a separate user. Performance issues can result if you fail to monitor the number of client registrations.

In the release 12.5(1)SU1, the IM and Presence Service supports Device Capacity Monitoring feature addresses performance issues by implementing additional counters to assist in monitoring the number of sessions created on the node.

Updated Counters:

The IM and Presence Service has been updated with the following counters to monitor the JSM sessions:

1. JsmClientSessionsActive
2. JsmPhantomSessionsActive
3. JsmHybridSessionsActive
4. JSMSessionsExceedsThreshold

For more information, see the "Device Capacity Monitoring" section in the *Configuration and Administration of the IM and Presence Service, Release 12.5SU1*.

Encrypted iX Channel for MRA

In this release, the Unified Communications Manager supports iX encryption negotiation for any SIP line devices. Unified CM can negotiate the DTLS information in secure active control messages for non-secure endpoints or softphones and receive messages. Sending Best effort iX encryption over TCP ensures Cisco IP Phones have an encrypted iX end to end.

For more information, see the "Encrypted iX Channel" section in the *Security Guide for Cisco Unified Communications Manager*.

FIPS Mode Support and Enhancement

Unified Communications Manager Release 12.5(1)SU1 supports Federal Information Processing Standards (FIPS) mode in Unified Communications Manager. FIPS is a U.S. and Canadian government certification standard that defines requirements that cryptographic modules must follow. Unified Communications Manager operates in FIPS 140-2 mode. When you enable FIPS 140-2 mode, Unified Communications Manager reboots, runs certification self-tests at startup, performs the cryptographic modules integrity check, and then regenerates the keying materials.

Following are the FIPS-enabled mode considerations and enhancements for this release:

- Upgrade Considerations—In Unified Communications Manager, the IPsec policies with DH group key values 1, 2 or 5 are disabled. In a FIPS-enabled mode, you have to delete the previously configured IPsec policies and perform the upgrade. After the upgrade is complete, reconfigure the IPsec policies with DH group key values from 14–18.

  For more information, see the "Upgrade Considerations with FIPS Mode" section of the *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service*.

- Security Password Restriction—Before you upgrade using FIPS-enabled mode, make sure that the security password length is greater than or equal to 14 characters to meet FIPS compliance.

- Certificate Key Length Restriction—Before you upgrade using FIPS-enabled mode, make sure that the certificates such as Tomcat, CallManager, and IPsec should have at least 2048-bits key length to perform a successful upgrade.
- Certificate Encryption Support Using Hashing Algorithm—In FIPS-enabled mode, certificates are encrypted using SHA-256 hashing algorithm. When you generate a self-signed certificate or Certificate Signing Request, you can choose only SHA-256 as the hashing algorithm, because SHA-1 is not supported.

  For more information, see the "FIPS 140-2 Mode Setup" chapter of the *Security Guide for Cisco Unified Communications Manager*.

FIPS for Outlook Calendar Integration

This release 12.5(1)SU1, the IM and Presence Service supports FIPS for Outlook Calendar Integration, A new service parameter for Cisco Presence Engine service **FIPS Mode Exchange Server Authentication** is introduced to validate the type of authentication used by the Presence Engine to establish a connection with Exchange Server through the Microsoft Outlook Calendar Integration feature.

You can set the FIPS Mode Exchange Server Authentication service parameter to either **Auto** or **Basic Only**, based on which the Presence Engine negotiates NTLMv1, NTLMv2 and Basic Authentication.

For more information, see the "FIPS for Outlook Calendar Integration" section in the *Configuration and Administration of the IM and Presence ServiceService, Release 12.5SU1*.

Gateway SIP Line Support

In this release, you can configure Analog FXS ports to communicate with Unified Communication Manager using the SIP protocol as a SIP endpoint. This configuration supports the same features on an analog phone that is currently available when the FXS port is configured as an SCCP endpoint. The system inserts a two-character string, AN (Analog), before the MAC address to indicate the phone device type when the analog phone is added to the FXS port.

This feature enhances the gateway functionality in Unified Communication Manager to support SIP protocol. VG450 and ISR 4461 gateways now support SIP protocol for SIP FXS analog ports. Analog phones must have similar core telephony features as a Cisco IP phone that is registered to Unified CM.

User Interface Updates

- To add VG450 and ISR 4461 gateways, choose **Cisco Unified CM Administrator** > **Bulk Administration** > **Gateways** > **Insert Gateways**.
- To import/export VG450 and ISR4461 SIP gateways, choose **Cisco Unified CM Administrator** > **Bulk Administration** > **Import/Export**. You can import the text file generated through BAT excel template. For example, bat.xlt.file.

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

About Headset Management

You can centrally manage Cisco Headsets configuration, firmware, inventory, troubleshooting, and diagnostic from Unified Communications Manager.

In Cisco Unified CM Administration, you can:

- Remotely configure the headset settings such as wireless power range, audio bandwidth, Bluetooth on/off, and more using Headset Templates.
- Define and control the firmware running on the headset.
- Get a detailed inventory of all the headsets in your deployment.
- Diagnose and troubleshoot headsets using Remote PRT, headset metrics in Call Management Records (CMR) and alarms.

Cisco Headset Service

Cisco Headset Service enables you to manage inventory, configuration updates, and diagnostics data of your Cisco Headset if you use compatible Cisco IP Phones or Cisco Jabber devices. You should enable this service in the **Cisco Unified Serviceability** user inteface to use the headset services.

For more information on the headset service, see the "Cisco Headset Service" section of the *Cisco Unified Serviceability Administration Guide, Release 12.5(1)SU1*.

Headset Template Important Considerations

The configuration changes introduced on Unified Communications Manager are not automatically configured on the Cisco Headsets. The Unified Communications Manager configurations are applied on Cisco Headsets only during the following scenarios:

1. Enable Cisco Headset Service—Administrators can see the Standard Default Headset Configuration Template (default template) only when the Cisco Headset Service is enabled. From this default template, you can create Custom Headset Configuration Templates and assign User Profiles to be used with this headset template as per your deployment needs and save the configuration changes.
2. Perform **Apply Config** on the Custom Headset Configuration Template so that the custom settings are applied on the headsets.
3. Perform **Apply Config** on the Standard Default Headset Configuration Template. Devices owned by end users associated with User Profiles in Assigned User Profile list and all anonymous devices will receive the default standard template settings.

For more information, see the “Headset Management” chapter in the *Feature Configuration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU1*.

Session Identifier in Call Detail Records

In this release, two new fields are introduced in CDR and CMR records. The session IDs of originating and terminating devices are recorded in CDR and CMR files.

Following are the new CDR and CMR fields:

CDR

- origDeviceSessionID (of type String)
- destDeviceSessionID (of type String)

CMR

- localSessionID (of type String)
- remoteSessionID (of type String)

For more information on the field description, see "CDR Field Descriptions" and “CMR Field Descriptions” section of the *Call Reporting and Billing Administration Guide for Cisco Unified Communications Manager*.

SIP OAuth Enhanced Security for MRA

In this release, the SIP OAuth Mode feature is enhanced to include a mutually authenticated TLS connection to Expressway-C from Cisco Unified Communications Manager Administration user interface. This configuration is required for devices in Mobile and Remote Access mode with SIP OAuth. For example, to enable Expressway registered B2B callers or endpoints to communicate with Unified CM registered endpoint.

For information on how to configure SIP OAuth Mode, see the "Configure SIP OAuth Mode" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU1*.

User Interface Updates

As a part of this feature, the **Expressway-C** configuration window has been added. You can access the feature from **Unified CM Administration** > **Device** > **Expressway-C**. This window contains the following fields that you must configure when deploying SIP OAuth Mode.

- Host Name/IP Address
- Description
- X509 Subject Name/Subject Alternate Name

Smart Licensing Export Compliance

Unified Communications Manager Restricted Software version is capable of strong encryption and is under U.S. Federal Export Regulation. To run Unified Communications Manager versions 12.0.x or 12.5.x in mixed-mode, it is necessary to successfully register the Unified Communications Manager with a "restricted" Registration Token from a Smart Account and Virtual Account.

From Release 12.5(1)SU1 release onwards, export restricted customers who are not able to generate a "restricted" Registration Token can order an Export Restricted Key and fulfill in Smart Account and Virtual Account to which the Unified Communications Manager is registered. Mixed-mode can be enabled after the completion of 'Request Export Key' operation from Unified Communications Manager. The Export Restricted Key is per instance of Unified Communications Manager and is associated with it after the completion of "Request Export Key".

Note Satellite deployment does not support Export Restricted Key functionality. Customers need to register their Unified Communications Manager directly or through Proxy to Cisco Smart Software Manager and complete the "Request Export Key" operation from Unified Communications Manager.

For details on how to configure Cisco Smart Licensing Export Compliance, see the “Specific License Reservation” chapter of the *System Configuration Guide for Cisco Unified Communications Manager*.

CLI Updates

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

- license smart export request local <exportfeaturename>
- license smart export return local <exportfeaturename>
- license smart export cancel

For more details about these CLI commands, see the “ License Commands” chapter of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Video Endpoints Management Overview

This feature simplifies the administrator's job of provisioning and managing Cisco TelePresence video endpoints. An administrator can provision settings for Cisco TelePresence endpoints in Unified Communications Manager and then push those Product-Specific Configuration settings to endpoints.

Prior to Release 12.5(1)SU1, only a limited set of Product-Specific Configurations were pushed from Unified Communications Manager to the endpoint resulting in a partial configuration of the endpoint. Administrator had to rely on Cisco TelePresence Management Suite or TelePresence Endpoint's web interface to configure all the settings. The Phone Configuration window in Unified Communications Manager contains a complete Product-Specific Configuration layout for Cisco TelePresence endpoints that matches what users see on their endpoint. This update lets administrators apply settings on behalf of users and then push those settings to users.

Note The Bulk Administration Tool (BAT) **Phone Template Configuration** page also displays the new model-specific configurations in a tabbed layout, supporting the complete list of endpoint parameters. You can import the entire set of parameters or modify a specific parameter in the endpoint in bulk.

Video endpoints managements feature provides the following benefits:

- TelePresence endpoints can be fully provisioned from Unified Communications Manager—Endpoints parameters listed in the Unified Communications Manager user interface are in the same order as listed in the **Advanced Configuration** settings of your Cisco TelePresence model. For more information on the various advanced parameters, see the respective model in the Collaboration Endpoints Administrator Guides.
- New **Product-Specific Configuration** Layout—New layout details the model-specific configurations in a tabbed layout. This is an upgrade from the earlier flat format that provided access only to a limited

set of parameters. The new layout ensures that you have a complete list of Cisco TelePresence settings on the Cisco Unified CM Administration interface.

- Automatic migration of the configuration data from the video endpoints—This simplifies the deployment of endpoints by automatically synching data from endpoints to Unified Communications Manager and vice versa. Endpoint configurations can be fully restored in case of reset to factory settings or Product Returns & Replacements (RMA) swaps.

Note Any endpoint that supports Collaboration Endpoint (CE) Software 9.8 or higher can use this new provisioning layout for the Product-Specific Configuration fields on the Phone Configuration page. If you are using a CE software version prior to 9.8, you will be able to view all the new set of advanced parameters; but, the new set of parameters functions only if you upgrade your CE Software version to 9.8 or higher. The subset of parameters supported is marked with a "#" to the right of each parameter value in the user interface. You must load a device pack onto Unified Communications Manager if a device type is capable of supporting the new provisioning framework, but does not show the additional parameters.

Provisioning and Migration Scenarios

The following table describe various provisioning and migration scenarios. All of these scenarios assume that your CE endpoints are upgraded to a CE release that supports Product-Specific Configuration provisioning from Unfiied CM. In Unified CM, these settings appear in the **Product-Specific Configuration** section, but on the endpoint, they appear under **Advanced Configuration**.

Table 1: Provisioning and Migration Scenarios for Video Endpoints

Task	Existing Configuration Summary	What to do
Provisioning New Video Endpoints	• Brand new device • Device is not provisioned on Unified CM • No existing settings on the device or on Unified CM	With Unified CM at a minimum release 12.5(1)SU1 and the CE endpoint at 9.8, you can provision new endpoints and manage the product-specific configurations from Unified CM.

Task	Existing Configuration Summary	What to do
Migrating Existing Video Endpoints from VCS	• Existing device • Device is not provisioned on Unified CM • Device is configured, but Unified CM does not have any of the configurations	If you are migrating existing video endpoints from a Cisco TelePresence Video Communications Server to Cisco Unified Communications Manager: **Adding Phones via Phone Configuration window in Unified CM:** • Add the phone to Unified CM, but DO NOT CLICK **Save**. • Register the phone. After registration, the existing **Advanced Configuration** settings from the phone are uploaded to Unified CM and display in **Product-Specific Configurations** in the **Phone Configuration** window. • In the **Phone Configuration** window, configure the new settings and click **Save**. The provisioned settings download to the phone. **Adding Phones via Bulk Administration** Make sure that the csv file or BAT Template that you use for provisioning does not include the Product-Specific Configuration fields. **Adding Phones via AXL** Make sure that the AXL request does not include any Product-Specific Configuration fields.
Upgrading from an Earlier Release of Unified CM with Registered Video Endpoints	• Existing device • Device is provisioned on a pre-12.5 release of Unified CM • Unified CM has a limited set of Product-Specific Configuration settings for the device	So long as the CE endpoint is at a supported version, when you upgrade Unified CM, the **Advanced Configuration** settings from the endpoint get pulled into Unified CM automatically following device registration and display under the **Product-Specific Configuration** section of the **Phone Configuration** window. After registration, you can set the **Configuration Control Mode** in addition to whatever settings you want.

Additional Information

For additional details, including procedures for migrating video endpoints from a Cisco TelePresence Video Communications Server to Cisco Unified Communications Manager, refer to the "Video Endpoints Management" chapter in the *Feature Configuration Guide for Cisco Unified Communications Manager*.