Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1)SU1

First Published: 2019-06-19

Last Modified: 2020-12-13

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1 **About this Release** 1

About Release Notes 1

Supported Versions 1

Documentation for this Release 1

Documentation Restructure 12.5(1)SU1 and Later 1

Open Source Documentation 3

Installation Procedures 3

Upgrade Procedures 3

Spectre/Meltdown Vulnerabilities During Upgrade 4

CHAPTER 2 **New and Changed Features** 5

MRA Device Onboarding using Activation Codes 5

Change in SHA-1 or MD5 Algorithm Values 7

CTI Monitoring 7

Device Capacity Monitoring 7

Encrypted iX Channel for MRA 8

FIPS Mode Support and Enhancement 8

FIPS for Outlook Calendar Integration 9

Gateway SIP Line Support 9

About Headset Management 10

Session Identifier in Call Detail Records 10

SIP OAuth Enhanced Security for MRA 11

Smart Licensing Export Compliance 11

Video Endpoints Management Overview 12

Provisioning and Migration Scenarios 13

CHAPTER 3 **Important Notes** 15

Blue Screen Appears for Unified CM Refresh Upgrades 15
Default CA Certificates During New Install and Upgrades 16
Disabled Default Certificates Backup Fails 16
ILS Networking Capacities 16
Java Requirements for SAML SSO Login to RTMT via Okta 17
Multiple Clock-Rates Not Supported in Same Call 17
New Cisco Gateway Support 17
SDL Listening Port Update Requires CTIManager Restart on all Nodes 18
Upgrade Database Schema from IM and Presence Release 11.5(1) and Above 19
Video Endpoint Migration Requirements 19
Restart Cisco Tomcat Service 20

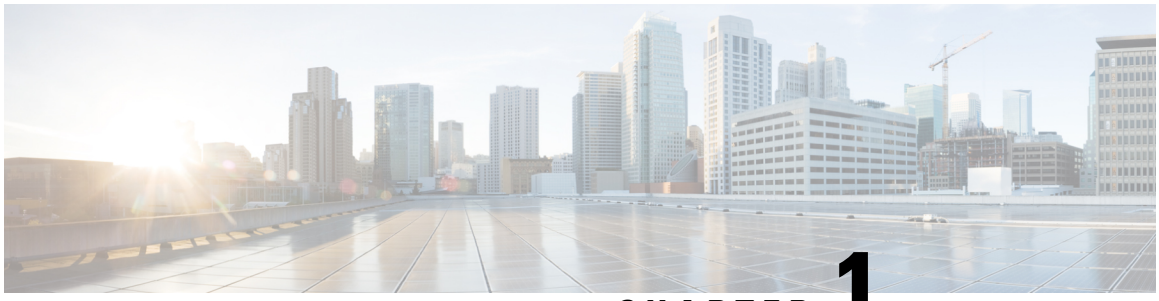
CHAPTER 4 **Caveats** 21

Bug Search Tool 21
Caveats for 12.5(1)SU1 22

CHAPTER 5 **Cisco Endpoints** 23

Cisco IP Phones and Gateways 23
Phone and Gateway Firmware Versions 23
Phone Firmware Releases on Cisco Unified Communication Manager 24
Phone Documents in Cisco Unified Communications Manager Self Care Portal 24
Deprecated Phone Models for Cisco Unified Communications Manager 24
IPv6-Only Impact on Cisco IP Phones with SCCP Firmware 25
Cisco Unified SIP Phone 3905 Features 25
Cisco Unified IP Phone 6900 Series Features 26
Cisco IP Phone 7800 Series Features 26
Cisco IP Conference Phone 7832 Features 26
Cisco Unified IP Phone 7900 Series Features 27
Cisco Unified Wireless IP Phone 7920 Series Features 27
Cisco IP Phone 8800 Series Features 27
Cisco Wireless IP Phone 8821 Features 28
Cisco Unified IP Conference Phone 8831 Features 29

Cisco IP Conference Phone 8832 Features 29
Cisco Unified IP Phone 8941 and 8845 Features 30
Cisco Unified IP Phone 8961, 9951, and 9971 Features 30
Cisco ATA 190 Series Features 30



CHAPTER 1

About this Release

- About Release Notes, on page 1
- Supported Versions, on page 1
- Documentation for this Release, on page 1
- Installation Procedures, on page 3
- Upgrade Procedures, on page 3

About Release Notes

This release describes new features, restrictions, and caveats for Cisco Unified Communications Manager (Unified Communications Manager) and Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service). The release notes are updated for every maintenance release but not for patches or hot fixes.

Supported Versions

The following software versions apply to Release 12.5(1)SU1:

- Unified Communications Manager 12.5.1.11900-146
- IM and Presence Service 12.5.1.11900-117

Documentation for this Release

For a complete list of the documentation that is available for Release 12.5(1)SU1, see the *Documentation Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1)* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/docguide/12_5_1/cucm_b_documentation-guide-cucm_imp_1251.html.

Documentation Restructure 12.5(1)SU1 and Later

Following is a summary of the documentation restructure effort that was a part of 12.5(1)SU1. For this release and later releases, many Unified Communications Manager documents were restructured in order to improve usability and to streamline the documentation set. As part of this effort, one new guide is added, three existing

guides are reworked, and five existing guides are deprecated. This overall effort reduces the size of the Unified Communications Manager documentation suite by four guides.

Table 1: Restructured Documents for 12.5(1)SU1 and Later

Restructured Documents	Description
System Configuration Guide	As of 12.5(1)SU1, the *System Configuration Guide* is shortened and streamlined to create a complete post-install system setup. Basic security and SSO configurations are added to fill out the basic setup, while advanced call processing features are moved to the *Feature Configuration Guide*. This new guide forms the Unified Communications Manager prerequisite for deploying an advanced Cisco call processing solution.
Feature Configuration Guide	This guide is expanded as the following advanced call processing topics are moved to this guide from the *System Configuration Guide*: • Call Control Discovery • External Call Control • Call Queuing • Call Throttling • Logical Partitioning • Location Awareness • Flexible DSCP Marking and Video Promotion • SIP Normalization and Transparency • SDP Transparency Profiles • Mobile and Remote Access In addition, the following new sections are added for 12.5(1)SU1 and later: • Headsets Managements • Video Endpoints Management
Administration Guide	As of 12.5(1)SU1, the *Administration Guide for Cisco Unified Communications Manager* is expanded to include consolidated administration information from the *Changing the IP Address, Hostname and Domain*document, the *Cisco Unified Reporting Administration Guide* document and many sections from the existing *Cisco Unified Serviceability Administration Guide* documentation, all of which are deprecated for 12.5(1)SU1 and later. In addition to the above updates, an overview of troubleshooting information has been inserted into the *Administration Guide*.
Call Reporting and Billing Administration Guide	This new document simplifies call reporting and billing administration documentation, consolidating existing material from the documents *Cisco Unified CDR Analysis and Reporting Administration Guide* and the *Call Detail Records Administration Guide*, both of which are now deprecated. It also adds CDR Repository and billing server information that was available previously with the Serviceability documentation. The new guide simplifies the overall structure and provides a clearer setup process:

Table 2: Restructured Documents for 12.5(1)SU3 and Later

Restructured Documents	Description
Security Guide	The Security Guide is restructured for Release 12.5(1)SU3. The new guide is streamlined and enhanced to make it easy to configure and deploy security for Unified Communications Manager and registered endpoints. The new guide is split into three sections: • **Basic Security**—Contains information on how to configure basic security on Unified Communications Manager and on registered endpoints. • **User Security**—Contains information on how to manage identity, authentication, and user access. • **Advanced Security Features**—Contains information on how to deploy advanced security features such as FIPS Mode, Enhanced Security Mode, and V.150. The book also includes enhanced information with new topics on subjects like Security Hardening and Identity Management that help you make security decisions for your deployment.
Push Notifications Deployment for Cisco Jabber on iPhone and iPad	This document describes how to configure Push Notifications for Cisco Jabber on iPhone and iPad with Cisco Unified Communications Manager and the IM and Presence Service. The guide is updated to include Push Notifications support for Cisco Jabber and Cisco Webex clients that run on both Android devices and iOS devices.

Open Source Documentation

This guide details the latest licenses and notices for the open source software used in Unified Communications Manager.

For more information on the open source softwares used, see https://www.cisco.com/c/dam/en_us/about/doing_business/open_source/docs/UnifiedCommunicationsManagerRelease1251SU2125v10.pdf.

Installation Procedures

For information on how to install your system, see the Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1).

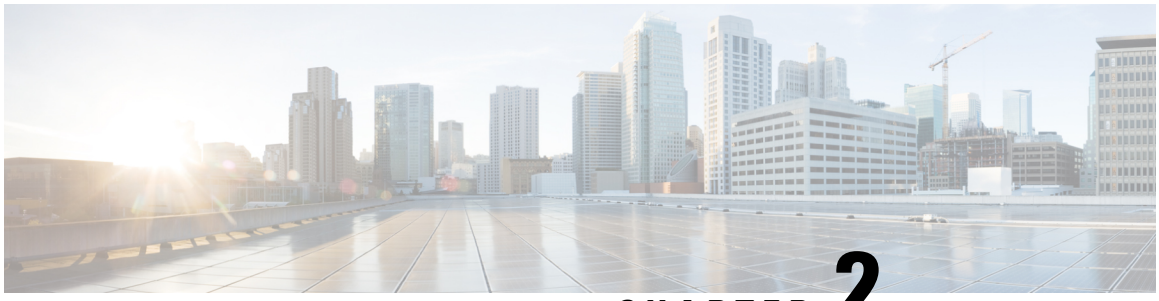
Upgrade Procedures

For information on how to upgrade to this release, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service, Release 12.5(1).

Spectre/Meltdown Vulnerabilities During Upgrade

This release of Unified Communications Manager, Cisco IM and Presence Service, Cisco Emergency Responder, and Cisco Prime Collaboration Deployment contain software patches to address the Meltdown and Spectre microprocessor vulnerabilities.

Before you upgrade to Release 12.5(1) or above, we recommend that you work with your channel partner or account team to use the Cisco Collaboration Sizing Tool to compare your current deployment to an upgraded deployment. If required, change VM resources to ensure that your upgraded deployment provides the best performance.



CHAPTER 2

New and Changed Features

- MRA Device Onboarding using Activation Codes, on page 5
- Change in SHA-1 or MD5 Algorithm Values, on page 7
- CTI Monitoring, on page 7
- Device Capacity Monitoring, on page 7
- Encrypted iX Channel for MRA , on page 8
- FIPS Mode Support and Enhancement, on page 8
- FIPS for Outlook Calendar Integration, on page 9
- Gateway SIP Line Support, on page 9
- About Headset Management, on page 10
- Session Identifier in Call Detail Records , on page 10
- SIP OAuth Enhanced Security for MRA, on page 11
- Smart Licensing Export Compliance, on page 11
- Video Endpoints Management Overview, on page 12

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**.

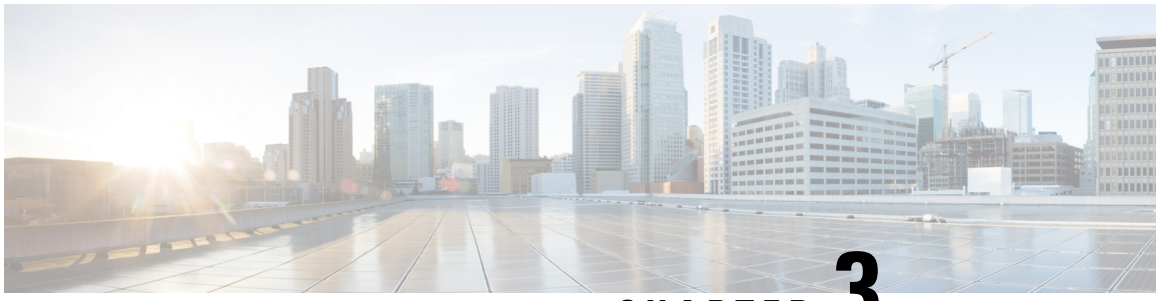
Table 3: Provisioning and Migration Scenarios for Video Endpoints

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*.



CHAPTER 3

Important Notes

- Blue Screen Appears for Unified CM Refresh Upgrades, on page 15
- Default CA Certificates During New Install and Upgrades, on page 16
- Disabled Default Certificates Backup Fails, on page 16
- ILS Networking Capacities, on page 16
- Java Requirements for SAML SSO Login to RTMT via Okta, on page 17
- Multiple Clock-Rates Not Supported in Same Call, on page 17
- New Cisco Gateway Support, on page 17
- SDL Listening Port Update Requires CTIManager Restart on all Nodes, on page 18
- Upgrade Database Schema from IM and Presence Release 11.5(1) and Above, on page 19
- Video Endpoint Migration Requirements, on page 19
- Restart Cisco Tomcat Service, on page 20

Blue Screen Appears for Unified CM Refresh Upgrades

An issue exists with refresh upgrades of Unified Communications Manager to specific destination releases. After the timezone data populates, you may see a blue transition screen appear for 30 minutes or more.

If you see this blue screen, DO NOT stop the upgrade, or a kernel panic occurs. The upgrade will continue to run even while the blue screen displays. The blue screen will clear itself after approximately 30 minutes

Affected 'To' Versions

This issue affects refresh upgrades of Unified Communications Manager where the destination version falls within the range in the below table. This range includes SU and ES versions that lay within the range. This issue does not occur for upgrades to older or newer versions that do not fall within the range, or for upgrades of the IM and Presence Service.

Table 4: Affected 'To' Versions for Blue Screen Refresh Upgrade Issue

Release Category	Affected Upgrade Destination Range
10.5(x)	10.5.2.21170-1—10.5.2.22188-1 (includes 10.5(2)SU9)
11.5(x)	11.5.1.16099—11.5.1.17118-1 (includes 11.5(1)SU6)
12.0(x)	12.0.1.23036-1 — 12.0.1.24053-1 (includes 12.0(1)SU3)

Release Category	Affected Upgrade Destination Range
12.5(x)	12.5.1.11001-1 — 12.5.1.12018-1 (includes 12.5(1)SU1)

For additional details, see CSCvs28202.

Default CA Certificates During New Install and Upgrades

After you install Unified Communications Manager Release 12.5(1) and above, all of the default CA certificates except for the CAP_RTP_001 and CAP_RTP_002 certificates are present. You can enable these certificates using the **set cert default-ca-list enable { all | common-name }** command.

If you are upgrading to Unified Communications Manager Release 12.5(1) and above, only the default certificates that were present in the older version appear after the upgrade.

Disabled Default Certificates Backup Fails

When you perform a backup using Disaster Recovery System (DRS), if all or specific default certificates are disabled using **set cert default-cal-list disable {all | common-name}**, then backup does not contain disabled certificates. When you are restoring the backup on the fresh installed server, those disabled certificates reappear.

ILS Networking Capacities

The Intercluster Lookup Service (ILS) network capacities have been updated for Release 12.5(x) and up. Following are the recommended capacities to keep in mind when planning an ILS network:

- ILS networking supports up to 10 hub clusters with 20 spoke clusters per hub, up to a 200 total cluster maximum. A hub and spoke combination topology is used to avoid many TCP connections created within each cluster.
- There may be a performance impact with utilizing your hub and spoke clusters at, or above, their maximums. Adding too many spoke clusters to a single hub creates extra connections that may increase the amount of memory or CPU processing. We recommend that you connect a hub cluster to no more than 20 spoke clusters.
- ILS networking adds extra CPU processing to your system. When planning your hub and spoke topology, make sure that your hub clusters have the CPU to handle the load. It may be a good idea to allocate systems with high CPU utilization as spoke clusters.

Note The above capacities are recommendations only, based on system testing. Unified Communications Manager does not enforce a limit, either on the total number of clusters in an ILS network, or on the number of spoke clusters per hub. The above topology is tested to ensure optimum performance so that the system does not burn too many resources.

For additional information on ILS, see the 'Configure Intercluster Lookup Service' chapter in the System Configuration Guide for Cisco Unified Communications Manager.

Java Requirements for SAML SSO Login to RTMT via Okta

If you have SAML SSO configured with Okta as the identity Provider, and you want to use SSO to log in to the Cisco Unified Real-Time Monitoring Tool, you must be running a minimum Java version of 8.221. This requirement applies to 12.5(x) releases of Cisco Unified Communications Manager and the IM and Presence Service.

Multiple Clock-Rates Not Supported in Same Call

With this release, Cisco TelePresence endpoints and Cisco Jabber clients do not support multiple "Telephone-Event" SDP attributes with different clock rates to match the offered codecs. This capability is required to interwork with VoLTE/IMS endpoints fully. Due to this update, interoperability issues between these endpoint types and VoLTE or IMS endpoints may arise for mid-call reinvites where a different clock rate from 8 kHz is negotiated.

For calls between these endpoint classes:

- The initial call setup occurs without any issues.
- Mid-call Re-INVITE will see no issues if the invite is initiated by Unified Communications Manager.
- Endpoint-initiated reinvites may see interoperability issues if they use a different clock-rate than 8 kHz.

New Cisco Gateway Support

New releases of Unified Communications Manager have introduced support for the following Cisco gateways:

- Cisco VG400 Analog Voice Gateway
- Cisco VG420 Analog Voice Gateway
- Cisco VG450 Analog Voice Gateway
- Cisco 4461 Integrated Services Router

The following table lists supported gateway models and the initial release, by release category, where support was introduced. Within each release category (for example, 11.5(x) and 12.5(x)), support for the gateway model is added as of the specified release, along with later releases in that category. For these releases, you can select the gateway in the **Gateway Configuration** window of Unified Communications Manager.

Table 5: Cisco Gateways with Initial Release By Release Category

Gateway Model	11.5(x) Releases	12.5(x) Releases	14(x) Releases
Cisco VG 202, 202 XM, 204, 204 XM, 310, 320, 350 Analog Voice Gateway	11.5(1) and later	12.5(1) and later	14 and later

Gateway Model	11.5(x) Releases	12.5(x) Releases	14(x) Releases
Cisco VG400 Analog Voice Gateway	11.5(1)SU7 and later	12.5(1) and later	14 and later
Cisco VG420 Analog Voice Gateway	Not supported	12.5(1)SU4 and later	14SU1 and later
Cisco VG450 Analog Voice Gateway	11.5(1)SU6 and later	12.5(1) and later	14 and later
Cisco 4321, 4331 4351, 4431, 4451 Integrated Services Router	11.5(1) and later	12.5(1) and later	14 and later
Cisco 4461 Integrated Services Router	11.5(1)SU6 and later	12.5(1) and later	14 and later
Cisco Catalyst 8300 Series Edge Platforms	—	12.5(1)SU4 and later	14 and later

Cisco Analog Telephone Adapters

Cisco Analog Telephone Adapters connect analog devices, such as an analog phone or fax machine, to your network. These devices can be configured via the **Phone Configuration** window. The following table highlights model support for the ATA series.

Table 6: Cisco Analog Telephone Adapters

ATA Adapter	11.5(x) Releases	12.5(x) Releases	14(x) Releases
Cisco ATA 190 Analog Telephone Adapter	11.5(1) and later	12.5(1) and later	14 and later
Cisco ATA 191 Analog Telephone Adapter	11.5(1)SU4 and later	12.5(1) and later	14 and later

SDL Listening Port Update Requires CTIManager Restart on all Nodes

If you edit the setting of the **SDL Listening Port** service parameter, you must restart the **Cisco CTIManager** service on all cluster nodes where the service is running. Currently, the help text says to restart the service, but does not specify that you must restart the service on all nodes where the service is running. You can access this service parameter from Cisco Unified CM Administration interface by navigating to **System** > **Service Parameters**, selecting **Cisco CTIManager** as the service, and clicking **Advanced** to see a complete list of CTIManager service parameters.

This update is a part of CSCvp56764.

Upgrade Database Schema from IM and Presence Release 11.5(1) and Above

If you have Microsoft SQL database deployed as an external database with the IM and Presence Service, choose either of the following scenarios to upgrade the database schema.

Table 7: MSSQL Database Schema Upgrade Scenarios

Scenario	Procedure
Upgrade from IM and Presence Service 11.5(1), 11.5(1)SU1, or 11.5(1)SU2 release	For more information on how to upgrade your MSSQL database, see the 'Database Migration Required for Upgrades with Microsoft SQL Server' section in the Database Setup Guide for the IM and Presence Service. This makes the necessary changes to the column types from TEXT to nvarchar(MAX).
Upgrade from IM and Presence Service 11.5(1)SU3 or later	The MSSQL database connected to the IM and Presence Service Server is upgraded automatically during IM and Presence Service upgrade. This makes the necessary changes to the column types from nvarchar(4000) to nvarchar(MAX). **Note** If you want to trigger an upgrade manually for any reason, such as to connect to an older database with column type as nvarchar(4000), the following actions trigger and upgrade the database by changing the column type to nvarchar(MAX): • Restarting Cisco XCP Config Manager followed by restarting Cisco XCP Router service; or • During schema verification of the external database—when you assign the database to Text Conferencing (TC), Message Archiver (MA) or Asynchronous File transfer (AFT) services, and reload the **External Database Settings** page. (From the Cisco Unified CM IM and Presence Administration user interface, choose **Messaging** > **External Server Setup** > **External Databases**, and then find and select the database to load the **External Database Settings** page.)

Video Endpoint Migration Requirements

If you are migrating Cisco TelePresence endpoints to any Cisco Unified Communications Manager 12.x release, it's highly recommended that you upgrade firmware to CE 9.8 or later before you migrate. Otherwise, Unified CM overwrites the existing endpoint configuration with default settings during device registration. This issue occurs because CE 9.7 and earlier does not have any method to communicate the existing configuration to Unified CM. If the endpoint is running CE 9.8 or higher, the endpoint sends the existing

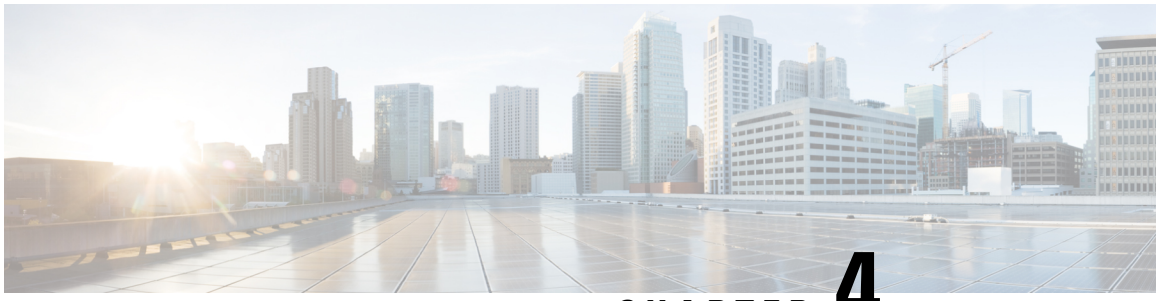
configuration to Unified Communications Manger during registration, thereby letting the administrator provision settings.

If you are registering existing TelePresence endpoints to a new Unified CM cluster, and maintaining the endpoint settings is required, make sure to use **Endpoint Configuration Mode** on Unified CM. Otherwise, Unfiied CM pushes its settings out to the endpoint. After you complete registration, you can change the configuration mode to whatever mode you want.

For procedures on how to migrate existing TelePresence endpoints to Cisco Unified Communications Manager, refer to the "Video Endpoints Management" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU1*.

Restart Cisco Tomcat Service

We recommend that you restart the Cisco Tomcat service after enabling or disabling Security Assertion Markup Language Single Sign-On (SAML SSO).



CHAPTER 4

Caveats

- Bug Search Tool, on page 21
- Caveats for 12.5(1)SU1, on page 22

Bug Search Tool

The system grades known problems (bugs) per severity level. These release notes contain descriptions of the following bug levels:

- All severity level 1 or 2 bugs
- Significant severity level 3 bugs
- All customer-found bugs

You can search for open and resolved caveats of any severity for any release using the Cisco Bug Search tool, an online tool available for customers to query defects according to their own needs.

To access the Cisco Bug Search tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Follow these steps to use Cisco Bug Search tool:

1. Access the Cisco Bug Search tool: https://tools.cisco.com/bugsearch/.
2. Log in with your Cisco.com user ID and password.
3. If you are looking for information about a specific problem, enter the bug ID number in the **Search for:** field and click **Go**.

Tip Click **Help** on the Bug Search page for information about how to search for bugs, create saved searches, and create bug groups.

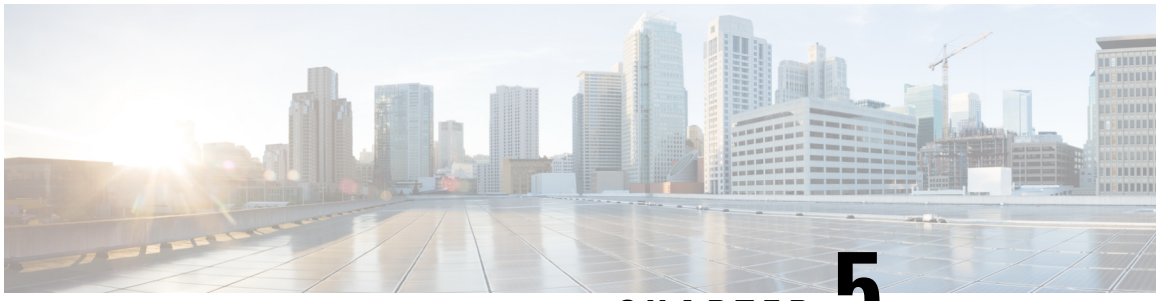
Caveats for 12.5(1)SU1

The following table compiles open caveats in this release. You can search for defects in the Bug Search Tool at https://bst.cloudapps.cisco.com/bugsearch/.

Caveats for 12.5(1)SU1

For a list of Open Caveats and Resolved Caveats, see the respective Readme files:

- ReadMe for Cisco Unified Communications Manager Release 12.5(1)SU1
- Read Me for Cisco Unified IM and Presence, Release 12.5(1)SU1



CHAPTER 5

Cisco Endpoints

• Cisco IP Phones and Gateways, on page 23

Cisco IP Phones and Gateways

Phone and Gateway Firmware Versions

The following table lists the latest Cisco IP Phone firmware versions supported for Cisco Unified Communications Manager 12.5(1).

Table 8: Phone Firmware Versions

Phone Family	Firmware Release Number
Cisco Unified SIP Phone 3905	9.4(1)SR3
Cisco Unified IP Phones 6901 and 6911	9.3(1)SR2
Cisco Unified IP Phones 6921, 6941, 6945, and 6961	9.4(1)SR3
Cisco IP Phone 7800 Series	12.5(1)
Cisco IP Conference Phone 7832	12.5(1)
Cisco Unified IP Phone 7900 Series	9.4(2)SR3
Cisco Unified Wireless IP Phones 7925G, 7925G-EX, and 7926G	1.4(8)SR1
Cisco IP Phone 8800 Series	12.5(1)
Cisco Wireless IP Phone 8821	11.0(4)SR1 11.0(5)
Cisco Unified IP Conference Phone 8831	10.3(1)SR4b
Cisco IP Conference Phone 8832	12.5(1)
Cisco Unified IP Phones 8941 and 8945	9.4(2)SR3

Phone Family	Firmware Release Number
Cisco Unified IP Phones 8961, 9951, and 9971	9.4(2)SR4

The following table lists the latest gateway firmware versions supported for Cisco Unified Communications Manager 12.5.

Table 9: Gateway Firmware Versions

Phone Family	Firmware Release Number
Cisco ATA 190 Analog Telephone Adapter	1.2.2
Cisco ATA 191 Analog Telephone Adapter	12.0(1)SR1

Phone Firmware Releases on Cisco Unified Communication Manager

Each Cisco Unified Communications Manager release contains a version of the phone firmware. But, this version may not be the latest version of the phone firmware.

The latest version of the phone firmware is available on the Software Download site.

Phone Documents in Cisco Unified Communications Manager Self Care Portal

The Cisco Unified Communications Manager Self Care Portal provide links to the IP Phone user guides in PDF format. These user guides are stored in the portal and match the phone firmware version that comes with the Cisco Unified Communications Manager release.

After a Cisco Unified Communications Manager release, subsequent updates to the user guides appear only on the Cisco website. The phone firmware release notes contain the applicable documentation URLs. In the web pages, updated documents display “Updated” beside the document link.

Note The Cisco Unified Communications Manager Device Packages and the Unified Communications Manager Endpoints Locale Installer do not update the English user guides on the Cisco Unified Communications Manager.

Administrators and users should check the Cisco website for updated user guides and download the PDF files. Administrators can also make the files available to the users on their company website.

Tip Administrators may want to bookmark the web pages for the phone models that are deployed in their company and send these URLs to their users.

Deprecated Phone Models for Cisco Unified Communications Manager

As of Cisco Unified Communications Manager Firmware Release 12.0 and later, the following phones are not supported:

- Cisco Unified IP Phone 7970G

- Cisco Unified IP Phone 7971G-GE
- Cisco Unified Wireless IP Phone 7921G

As of Cisco Unified Communications Manager Firmware Release 11.5 and later, the following phones are not supported:

- Cisco IP Phone 12 SP+ and related models
- Cisco IP Phone 30 VIP and related models
- Cisco Unified IP Phone 7902
- Cisco Unified IP Phone 7905
- Cisco Unified IP Phone 7910
- Cisco Unified IP Phone 7910SW
- Cisco Unified IP Phone 7912
- Cisco Unified Wireless IP Phone 7920
- Cisco Unified IP Conference Station 7935

IPv6-Only Impact on Cisco IP Phones with SCCP Firmware

In Cisco Unified Communications Manager Release 12.0, you can use IPv6 to communicate with the phones that run Session Initiation Protocol (SIP) firmware.

Some of the Cisco IP Phones can run with Skinny Client Control Protocol (SCCP) firmware. The SCCP firmware does not support IPv6. The following desk phones can run with either SIP or SCCP firmware:

- Cisco Unified IP Phone 6901, 6911, 6921, 6941, 6945, and 6961
- Cisco Unified IP Phone 7906G, 7911G, 7931G, 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7965G, 7962G, 7970G, 7971G-GE, and 7975G
- Cisco Unified IP Phone 8941 and 8945

If you set up your Cisco Unified Communications Manager to communicate in IPv6 only, any of above phones that have SCCP firmware installed must be upgraded to SIP firmware. The SCCP firmware cannot communicate with the Cisco Unified Communications Manager with IPv6.

The Cisco Wireless IP Phones 7925G, 7925G-EX, and 7926G are also SCCP phones. They do not have SIP firmware and only support IPv4.

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

Cisco Unified SIP Phone 3905 Features

No new features were introduced for the Cisco Unified SIP Phone 3905 in Firmware Release 9.4(1)SR3.

Cisco Unified IP Phone 6900 Series Features

No new features were introduced for the Cisco Unified IP Phones 6900 Series.

Cisco IP Phone 7800 Series Features

The following table lists the features added to the Cisco IP Phone 7800 Series for Firmware Releases 12.0(1), 12.1(1), 12.1(1)SR1, and 12.5(1). For more information, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-release-notes-list.html.

Feature Name	Firmware Release
IPv6 Feature Support	12.0(1)
Mobile and Remote Access Through Expressway and Domain Name Handling	12.0(1)
Cisco Headset 531 and Cisco Headset 532	12.1(1)
G722.2 ANR-WB Support	12.1(1)
Transport Layer Security Enhancements	12.1(1)
Enbloc Dialing	12.1(1)SR1
Activation Code Onboarding	12.5(1)
Cisco Headset 561 and 562	12.5(1)
Disable the Handset for Headset Users	12.5(1)
Disable Transport Layer Support Ciphers	12.5(1)
Elliptic Curve Support	12.5(1)
Interactive Connectivity Establishment and media Paths	12.5(1)
Remote Configuration of Headset Parameters	12.5(1)
Whisper Paging and Cisco Unified Communications Manager Express	12.5(1)

Cisco IP Conference Phone 7832 Features

The following table lists the features added to the Cisco IP Conference Phone 7832 for Firmware Releases 12.0(1),12.1(1), and 12.5(1). For more information, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7800-series/products-release-notes-list.html.

Feature Name	Firmware Release
Client Matter Code and Forced Authorization Code	12.1(1)
Mobile and Remote Access Through Expressway	12.1(1)
Transport Layer Security Enhancements	12.1(1)
Disable Transport Layer Support Ciphers	12.5(1)
Elliptic Curve Support	12.5(1)
Whisper Paging and Cisco Unified Communications manager Express	12.5(1)

Cisco Unified IP Phone 7900 Series Features

No new features were introduced for the Cisco Unified IP Phones 7900 Series.

Cisco Unified Wireless IP Phone 7920 Series Features

No new features were introduced for the Cisco Unified Wireless IP Phones 792x Series.

Cisco IP Phone 8800 Series Features

The following table lists the features added to the Cisco IP Phone 8800 Series for Firmware Releases 12.0(1), 12.0(1)SR1, 12.1(1), 12.1(1)SR1, and 12.5(1). For more information, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-release-notes-list.html.

Feature Name	Firmware Release
New Feature Support for Enhanced Line Mode	12.0(1)
IPv6 Feature Support	12.0(1)
Mobile and Remote Access Through Expressway and Domain Name Handling	12.0(1)
Key Expansion Modules for Cisco IP Phone 8851, 8851NR, 8861, 8865, and 8865NR	12.0(1)
Cisco Headset 531 and Cisco Headset 532	12.1(1)
Voice Feedback	12.1(1)
Call History Enhancements	12.1(1)
Incoming Calls and Enhanced Line Mode	12.1(1)
Speed Dial and Navigation Enhancements	12.1(1)

Feature Name	Firmware Release
G722.2 ANR-WB Support	12.1(1)
Transport Layer Security Enhancements	12.1(1)
Enhanced Line Mode and Simplified Line Display for Incoming Calls	12.1(1)SR1
Wallpaper and Key Expansion Modules	12.1(1)SR1
Enbloc Dialing	12.1(1)SR1
Activation Code Onboarding	12.5(1)
Chinese Language Support	12.5(1)
Cisco Headset 561 and 562	12.5(1)
Disable the Handset for Headset Users	12.5(1)
Disable Transport Layer Support Ciphers	12.5(1)
Elliptic Curve Support	12.5(1)
Enhanced Line Mode and Call History	12.5(1)
Interactive Connectivity Establishment and Media Paths	12.5(1)
Remote Configuration of Headset Parameters	12.5(1)
Transport Layer Security 1.2 and Wireless Authentication	12.5(1)
Whisper Paging and Cisco Unified Communications Manager Express	12.5(1)

Cisco Wireless IP Phone 8821 Features

The following table lists the features added to the Cisco Wireless IP Phone 882x Series for Firmware Releases 11.0(3)SR4, 11.0(3)SR5, 11.0(3)SR6, 11.0(4), 11.0(4)SR1, and 11.0(4)SR2. For more information, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-release-notes-list.html.

Feature Name	Firmware Release
OPUS Codec Support	11.0(3)SR4
Bulk Deployment Utility	11.0(3)SR4
Configurable Home Screen	11.0(4)
Local Contacts	11.0(4)

Feature Name	Firmware Release
Problem Report Tool	11.0(4)
Ringtone Enhancements	11.0(4)
User Interface Enhancements for Firmware Release 11.0(4)	11.0(4)
Resized Wallpapers	11.0(4)

Cisco Unified IP Conference Phone 8831 Features

No new features were introduced for the Cisco Unified IP Conference Phone 8831.

Cisco IP Conference Phone 8832 Features

The following table lists the features added to the Cisco Conference IP Phone 8832 for Firmware Releases 12.0(1)SR2, 12.0(1)SR3, 12.1(1) and 12.5(1). For more information, see the Release Notes at the following location: http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-release-notes-list.html.

Feature Name	Firmware Release
Cisco IP Conference Phone 8832 PoE Injector	12.0(1)SR2
Audio Clock Frequency	12.0(1)SR3
Client Matter Code and Forced Authorization Code	12.1(1)
Daisy Chain Support	12.1(1)
G722.2 ANR-WB Support	12.1(1)
Wireless Microphone Support	12.1(1)
Mobile and Remote Access Through Expressway	12.1(1)
Transport Layer Security Enhancements	12.1(1)
Wi-Fi Support and Wireless LAN Profiles	12.1(1)
Disable Transport Layer Support Ciphers	
Elliptic Curve Support	12.5(1)SR2
Transport Layer Security 1.2 and Wireless Authentication	12.5(1)SR2
Whisper Paging and Cisco Unified Communications Manager Express	12.5(1)SR2

Cisco Unified IP Phone 8941 and 8845 Features

No new features were introduced for the Cisco Unified IP Phone 8941 and 8945.

Cisco Unified IP Phone 8961, 9951, and 9971 Features

No new features were introduced for the Cisco Unified IP Phone 8961, 9951, and 9971.

Cisco ATA 190 Series Features

The Cisco ATA 190 Analog Telephone Adapter had no new features added.

The Cisco ATA 191 Analog Telephone Adapter was released after Cisco Unified Communications Manager 12.1 was released. This device allows you to turn an analog phone or fax machine into an IP phone. No new features were introduced after the initial release.