Cisco IP Conference Phone 7832 Release Notes for Firmware Release 12.5(1)SR2

First Published: 2019-03-25

Cisco IP Conference Phone 7832 Release Notes for Firmware Release 12.5(1)SR2

These release notes support the Cisco IP Conference Phone 7832 running SIP Firmware Release 12.5(1)SR2.

Note Firmware Release 12.5(1)SR2 replaces Firmware Release 12.5(1) and Firmware 12.5(1)SR1. Firmware Release 12.5(1) and Firmware Release 12.5(1)SR1 have been deferred in favor of Firmware Release 12.5(1)SR2.

The following table lists the support and protocol compatibility for the Cisco IP Phones.

Table 1: Cisco IP Phones, Support, and Firmware Release Compatibility

Cisco IP Phone	Protocol	Support Requirements
7832	SIP	Cisco Unified Communications Manager 10.5(2) and later Cisco Unified Communications Manager DST Olsen version D or later SRST 8.0 (IOS load 15.1(1)T) and above Cisco Expressway 8.7
7832	SIP	Unified CME 12.3 (Cisco IOS XE Fuji 16.9.1 release)

Related Documentation

Use the following sections to obtain related information.

Cisco IP Conference Phone 7832 Documentation

Refer to publications that are specific to your language and call control system. Navigate from the following documentation URL:

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-7800-series/index.html

Cisco Unified Communications Manager Documentation

See the *Cisco Unified Communications Manager Documentation Guide* and other publications that are specific to your Cisco Unified Communications Manager release. Navigate from the following documentation URL:

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

New and Changed Features Introduced in Firmware Release 12.5(1) and 12.5(1)SR1

In Firmware Release 12.5(1) and Firmware Release 12.5(1)SR1, we introduced the features in the following sections. No new features were introduced in Firmware Release 12.5(1)SR2.

Features Available with the Firmware Release

The following sections describe the features available with the Firmware Release.

Whisper Paging and Cisco Unified Communications Manager Express

Your users have an improved call experience with whisper paging. In previous releases, your calls were interrupted by a page. But now your phone rejects any pages when you are on a call, and ensures a distraction-free experience.

This feature is supported on Cisco Unified Communications Manager Express.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Administration Guide for Cisco Unified Communications Manager*

Activation Code Onboarding

You can use Activation Code Onboarding to quickly set up new phones without autoregistration. With this approach, you control the phone onboarding process using the one of the following:

- Cisco Unified Communications Bulk Administration Tool (BAT)
- Cisco Unified Communications Manager Administration interface
- Administrative XML Web Service (AXL)

Users must enter an activation code before their phones can register with Cisco Unified Communications Manager (CUCM). Activation Code Onboarding can be applied to individual phones, a group of phones, or across an entire network.

Administrators find this approach improves control because phones cannot register until the activation code is entered and the Manufacturing Installed Certificate (MIC) is verified. It is also a convenient way to bulk onboard phones because it doesn't use the Tool for Auto-registered Phone Support (TAPS) or autoregistration.

Activation Code Onboarding is an easy way for users to configure their phones because they only enter a 16-digit activation code. Codes are entered either manually or with a QR code if a phone has a video camera. An administrator provides the codes, or a user may be able to get one from the Self Care portal. But they expire after 1 week by default and an administrator regenerates a new one.

This feature is supported on phones that are used within a company's premises.

Activation Code Onboarding requires Cisco Unified Communications Manager 12.5(1) or later to function properly.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Administration Guide for Cisco Unified Communications Manager*
- *Cisco IP Conference Phone 7832 User Guide*

Elliptic Curve Support

Your Cisco IP Phone has been made even more secure with support for Elliptic Curve Digital Signature Algorithm (ECDSA) certificates. These certificates are stronger than the RSA-based certificates and require a smaller key size, making them a quicker solution for your network security.

The ECDSA certificates are available in the following areas—Certificate Manager, SIP, Certificate Authority Proxy Function (CAPF), Transport Layer Security (TLS) Tracing, Entropy, HTTP, and computer telephony integration (CTI) Manager.

Elliptic Curve Digital Signature Algorithm (ECDSA) certificates require Cisco Unified Communications Manager 12.5(1) or later.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Administration Guide for Cisco Unified Communications Manager*
- *Security Guide for Cisco Unified Communications Manager, Release 12.0(1)*

Interactive Connectivity Establishment and Media Paths

Mobile Remote Access (MRA) now supports Interactive Connectivity Establishment (ICE). ICE is an optional deployment that improves the reliability of MRA calls across a firewall or Network Address Translation (NAT). It uses Serial Tunneling and Traversal Using Relays around NAT services to select the best media path for a call.

ICE is configured in these ways:

- System defaults—You apply ICE settings across a network with the **Enterprise Phone Configuration** window.
- ICE Profiles—You apply ICE settings to a phone group with the **Common Phone Profile Configuration**.

Secondary Turn Server and Turn Server Failover is not supported.

You can find additional information in the Internet Engineering Task Force (IETF) Request for Comment documents:

- *Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)*(RFC 5766)
- *Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols* (RFC 5245)

Interactive Connectivity Establishment requires Cisco Unified Communications Manager 12.5(1) or later to function properly. Interactive Connectivity Establishment is also supported on Cisco Expressway X12.5 or later.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Administration Guide for Cisco Unified Communications Manager*

Features Available with the Latest Cisco Unified Communications Manager Device Pack

The following sections describe features in the release which require the new firmware and the latest Cisco Unified Communications Manager Device Pack.

For information about the Cisco Unified IP Phones and the required Cisco Unified Communications Manager device packs, see the following URL:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/devpack_comp_mtx.html

Disable Transport Layer Support Ciphers

You can now disable specific Transport Layer Support (TLS) cipher suites that are used by the TLS connection, or handshake between the network and a phone. This allows you to tailor your security for known vulnerabilities, and to align your network with your company's policies for ciphers.

You disable ciphers with the Disable TLS Ciphers parameter. Sign into Cisco Unified Communications Manager Administration, and navigate to **Device** > **Phones**. Select your phone, and navigate to the Disable TLS Ciphers field in the Product Specific Configuration Layout pane.

Your choices are:

- None
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

None is the default setting. If you select all of the phone ciphers, then phone TLS service is impacted.

For more information about phone ciphers and security, see *Cisco IP Phone 7800 and 8800 Series Security Overview* available at https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-listing.html

This feature has no user impact.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Administration Guide for Cisco Unified Communications Manager*

Enbloc Dialing

You can now place calls quicker with Enbloc Dialing. When enabled, this feature eliminates the delay often experienced when dialing a phone number during the following scenarios:

- On hook dialing and redialing
- Speed dial and Speed dial BLF
- Voice mail

- Calls that are made from your Recent list
- Calls that are made from your Directory

Previously users experienced a delay of up to 15 seconds when placing a call.

Administrators can find the Enbloc Dialing parameter in the Product Specific Configuration Layout section of the Cisco Unified Communications Manager. When enabled, it overrides the T.302 timer and the entire dialed string is sent to the Cisco Unified Communications Manager once the dialing is complete.

Forced Authorization Codes (FAC) or Client Matter Codes (CMC) do not support Enbloc Dialing. If you use FAC or CMC to manage call access and accounting, then you cannot use this feature.

Where to Find More Information

- *Cisco Collaboration System 12.x Solution Reference Network Designs*
- *Cisco IP Conference Phone 7832 Administration Guide for Cisco Unified Communications Manager*

Installation

Installation Requirements

Before you install the firmware release, you must ensure that your Cisco Unified Communications Manager is running the latest device pack. After you install a device pack on the Cisco Unified Communications Manager servers in the cluster, you need to reboot all the servers.

Note If your Cisco Unified Communications Manager does not have the required device pack to support this firmware release, the firmware may not work correctly.

For information on the Cisco Unified Communications Manager Device Packs, see http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/devpack_comp_mtx.html.

Install the Firmware Release on Cisco Unified Communications Manager

Before using the phone firmware release on the Cisco Unified Communications Manager, you must install the latest Cisco Unified Communications Manager firmware on all Cisco Unified Communications Manager servers in the cluster.

Procedure

Step 1 Go to the following URL:

https://software.cisco.com/download/navigator.html?mdfid=284883944&i=rm

Step 2 Choose **Cisco IP Phone 7800 Series**.

Step 3 Choose **IP Conference Phone 7832**.

Step 4 Choose **Session Initiation Protocol (SIP) Software**.

Step 5 In the Latest Releases folder, choose **12.5(1)SR2**.

Step 6 Select the firmware file, click the **Download** or **Add to cart** button, and follow the prompts.

The firmware filename is cmterm-7832-sip.12-5-1SR2-2.k3.cop.sgn.

Note If you added the firmware file to the cart, click the **Download Cart** link when you are ready to download the file.

Step 7 Click the + next to the firmware file name in the Download Cart section to access additional information about this file. The hyperlink for the readme file is in the Additional Information section, which contains installation instructions for the corresponding firmware.

Step 8 Follow the instructions in the readme file to install the firmware.

Install the Firmware Zip Files

If a Cisco Unified Communications Manager is not available to load the installer program, the following .zip file is available to load the firmware:

cmterm-7832.12-5-1SR2-2.zip

Firmware upgrades over the WLAN interface may take longer than upgrades using a wired connection. Upgrade times over the WLAN interface may take more than an hour, depending on the quality and bandwidth of the wireless connection.

Procedure

Step 1 Go to the following URL:

https://software.cisco.com/download/navigator.html?mdfid=284729655&flowid=75283

Step 2 Choose **Cisco IP Phones 7800 Series**.

Step 3 Choose **IP Conference Phone 7832**.

Step 4 Choose **Session Initiation Protocol (SIP) Software**.

Step 5 In the Latest Releases folder, choose **12.5(1)SR2**.

Step 6 Download the relevant zip files.

Step 7 Unzip the files.

Step 8 Manually copy the unzipped files to the directory on the TFTP server. See *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service* for information about how to manually copy the firmware files to the server.

Limitations and Restrictions

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone voice and in some cases can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- Administrative tasks, such as an internal port scan or security scan
- Attacks that occur on your network, such as a Denial of Service attack

Health-Care Environment Use

This product is not a medical device and uses an unlicensed frequency band that is susceptible to interference from other devices or equipment.

Language Limitation

There is no localized Keyboard Alphanumeric Text Entry (KATE) support for the following Asian locales:

- Chinese (China)
- Chinese (Hong Kong)
- Chinese (Taiwan)
- Japanese (Japan)
- Korean (Korea Republic)

The default English (United States) KATE is presented to the user instead.

For example, the phone screen will show text in Korean, but the **2** key on the keypad will display **a b c 2 A B C**.

Caveats

View Caveats

You can search for caveats using the Cisco Bug Search.

Known caveats (bugs) are graded according to severity level, and can be either open or resolved.

Before you begin

To view caveats, you need the following items:

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

Procedure

Step 1 Perform one of the following actions:

- To find all caveats for this release, use this URL:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286312831&rls=12.5(1)&sb=anfr&sts=open&svr=3nH&bt=custV

- To find all open caveats for this release, use this URL:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286312831&rls=12.5(1)&sb=afr&sts=open&svr=3nH&bt=custV

- To find all resolved caveats for this release, use this URL:

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286312831&rls=12.5(1),12.5(1.*)&sb=fr&sts=fd&svr=3nH&bt=custV

Step 2 When prompted, log in with your Cisco.com user ID and password.

Step 3 (Optional) To look for information about a specific problem, enter the bug ID number in the Search for field, and press **Enter**.

Open Caveats

Currently, there are no open defects for the Cisco IP Conference Phone 7832 for Firmware Release 12.5(1)SR2.

For more information about an individual defect, access the Bug Search toolkit and search for the defect using the Identifier. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, the table reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access the Bug Toolkit as described in View Caveats, on page 7.

Resolved Caveats

The following list contains severity 1, 2, and 3 defects that are resolved for the Cisco IP Phone 7832 Series for Firmware Release 12.5(1)SR2.

For more information about an individual defect, access the Bug Search toolkit and search for the defect using the Identifier. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, the table reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of resolved defects, access the Bug Toolkit as described in View Caveats, on page 7.

- CSCvn25400: java crashed during sharedline stress test
- CSCvn79514: No audible alert played for 7800/8800 IP phones when night service is enabled
- CSCvo39524: 88xx: Display screen ON cannot be set for the 24h and kept ON always
- CSCvo50891: 78xx Multiple Vulnerabilities in libxml2

The following list contains severity 1, 2, and 3 defects that are resolved for the Cisco IP Conference Phone 7832 for Firmware Release 12.5(1)SR1.

- CSCvn14646: CVE-2018-18559: Linux Kernel Use-After-Free Race Condition Vulnerability
- CSCvn47250: Phone crashes after receiving malformed CDP/LLDP data
- CSCvn54297: Slow user interface due to PAE process memory leak when 802.1x is enabled but not used
- CSCvn56168: Buffer overflow vulnerability in the phone webserver
- CSCvn56175: Authorization bypass in phone web interface
- CSCvn56213: Phone file upload path traversal and null injection vulnerability
- CSCvn56221: CSRF vulnerability in the phone upload function
- CSCvn57643: No ringback tone played after initial announcement

- CSCvn72978: IP Phone getting unregistered when using Alcatel Switch

The following table lists severity 1, 2, and 3 defects that are resolved for the Cisco IP Conference Phone 7832 for Firmware Release 12.5(1).

- CSCvh78212: No "Private" display on incoming call toast when CLIR is enable on.
- CSCvi33608: Unable to add phone number to PD entry if no numbers before

Cisco Unified Communication Manager Public Keys

To improve software integrity protection, new public keys are used to sign cop files for Cisco Unified Communications Manager Release 10.0.1 and later. These cop files have “k3” in their name. To install a k3 cop file on a pre-10.0.1 Cisco Unified Communications Manager, consult the README for the ciscocm.version3-keys.cop.sgn to determine if this additional cop file must first be installed on your specific Cisco Unified Communications Manager version. If these keys are not present and are required, you will see the error “The selected file is not valid” when you try to install the software package.

Unified Communications Manager Endpoints Locale Installer

By default, Cisco IP Phones are set up for the English (United States) locale. To use the Cisco IP Phones in other locales, you must install the locale-specific version of the Unified Communications Manager Endpoints Locale Installer on every Cisco Unified Communications Manager server in the cluster. The Locale Installer installs the latest translated text for the phone user interface and country-specific phone tones on your system so that they are available for the Cisco IP Phones.

To access the Locale Installer required for a release, access https://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245, navigate to your phone model, and select the Unified Communications Manager Endpoints Locale Installer link.

For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Note The latest Locale Installer may not be immediately available; continue to check the website for updates.

Cisco IP Phone Documentation Updates on Cisco Unified Communications Manager

The Cisco Unified Communications Manager Self Care Portal (Release 10.0 and later) and User Options web pages (Release 9.1 and earlier) provide links to the IP Phone user guides in PDF format. These user guides are stored on the Cisco Unified Communications Manager and are up to date when the Cisco Unified Communications Manager release is first made available to customers.

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.

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

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

Cisco IP Phone Firmware Support Policy

For information on the support policy for phones, see https://cisco.com/go/phonefirmwaresupport.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)