Cisco IP Conference Phone 7832 Release Notes for Firmware Release 14.0(1)

First Published: 2021-04-01

Cisco IP Conference Phone 7832 Release Notes for Firmware Release 14.0(1)

These release notes support the Cisco IP Conference Phone 7832 running SIP Firmware Release 14.0(1).

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

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

Cisco IP Phone	Support Requirements
7832	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	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

Features Available with the Firmware Release

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

User Interface Enhancements

This release contains the following enhancements to the phone user interface:

- When the phone is in Survivable Remote Site Telephony (SRST) mode, the phone can display a programmable line key with a Service URL.

Where to Find More Information

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

Hunt Group Enhancements

Hunt group enhancements:

- If a phone is part of a broadcast hunt group, calls picked up by other members of the hunt group display in call history as a Received call.

Where to Find More Information

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

COP File SHA-512 Enhancement

Beginning with Cisco Unified Communications Manager version 14.0, all phone loads must be encrypted with the SHA512 hashing algorithm and end with the file name `.cop.sha512`.

Where to Find More Information

Security Guide for Cisco Unified Communications Manager 14.0(1)

Security Enhancement

This release provides the following security enhancement:

Datagram Transport Layer Security (DTLS) 1.2 support.

Note DTLS 1.2 requires Cisco Adaptive Security Appliance (ASA) Release 9.10 or later. You configure the minimum DTLS version for a VPN connection in ASA.

DTLS 1.2 has no user or administrator impact.

Where to Find More Information

ASDM Book 3: Cisco ASA Series VPN ASDM Configuration Guide at https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

SIP OAuth Mode for Mobile and Remote Access Through Expressway

SIP OAuth mode is now supported for Mobile and Remote Access Through Expressway. This mode allows you to use OAuth access tokens for authentication in secure environments.

SIP OAuth mode is supported on Cisco Expressway release X14.0(1) and later, and Cisco Unified Communications Manager 14.0(1) and later.

Note For SIP OAuth in Mobile and Remote Access (MRA) mode, use only Activation Code Onboarding with Mobile and Remote Access when you deploy the phone. Activation with username and password is not supported.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Administration Guide*
- *Feature Configuration Guide for Cisco Unified Communications Manager* (Release 14.0(1) or later)

OAuth Enhancement

You can improve the security of your phones to use OAuth tokens to authenticate the phones. SIP lines with OAuth allow secure signalling and media.

The feature requires Cisco Unified Communications Manager Release 14.0(1) or later.

You enable the feature from the Cisco Unified Communications Manager Administration **System** > **Enterprise Parameters** page.

This feature has no user impact.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Administration Guide*
- *Feature Configuration Guide for Cisco Unified Communications Manager* (Release 14.0(1) or later)

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 Unified CM servers in the cluster, you need to reboot all the servers.

Note If your Cisco Unified Communications Manager doesn't 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 https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/matrix/CMDP_BK_CCBDA741_00_cucm-device-package-compatibility-matrix.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 your phone model.

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

Step 5 In the Latest Releases folder, choose **14.0(1)**.

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.14-0-1-0001-135.k3.cop.sha512

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

Step 7 Click the + next to the firmware file name in the File Information section to access additional information about this file. The hyperlink for the Readme file is in the Details 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-7832.14-0-1-0001-135_REL.zip

Procedure

Step 1 Go to the following URL:

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

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

Step 3 Choose your phone model.

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

Step 5 In the Latest Releases folder, choose **14.0(1)**.

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 *Cisco Unified Communications Operating System Administration Guide* 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 audio and video quality, 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 Tool.

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:

- Use this URL for all caveats:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=284883944&rls=14.0(1.*),14.0(1)&sb=anfr&svr=3nH&bt=custV

- Use this URL for all open caveats:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=284883944&rls=14.0(1)&sb=afr&sts=open&svr=3nH&bt=custV

- Use this URL for all resolved caveats:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=284883944&rls=14.0(1.*),14.0(1)&sb=fr&svr=3nH&bt=custV

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

Step 3 (Optional) Enter the bug ID number in the Search for field, then press **Enter**.

Open Caveats

There aren't any open bugs for Cisco IP Phone 7832 Series for Firmware Release 14.0(1).

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

Because bug status continually changes, the list reflects a snapshot of the caveats that were open at the time this report was compiled. For an updated view of open caveats, access the Bug Search Tool as described in View Caveats, on page 5.

Resolved Caveats

The following list contains severity 1, 2, and 3 caveats that are resolved for the Cisco IP Phone 7832 Series for Firmware Release 14.0(1).

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

Because bug status continually changes, the list reflects a snapshot of the caveats that were open at the time this report was compiled. For an updated view of resolved caveats, access the Bug Tool as described in View Caveats, on page 5.

- CSCvu59349 - Multiple BufferOverflow + Out of Bounds Read for LLDP and CDP
- CSCvt27644 - Cisco IP Phone Call Log Information Disclosure Vulnerability
- CSCvx59068 - IP Phone 7832 CDP Out-of-Bounds Read in Addresses TLV

Cisco IP Phone Firmware Support Policy

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

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.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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)