



Cisco IP Conference Phone 7832 Release Notes for Firmware Release 12.1(1)

First Published: 2018-04-20

Cisco IP Conference Phone 7832 Release Notes for Firmware Release 12.1(1)

These release notes support the Cisco IP Conference Phone 7832 running SIP Firmware Release 12.1(1). 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

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

The following sections describe the features that are new or have changed in this release.

**Note**

Some features may require the installation of a Cisco Unified Communications Manager Device Package. Failure to install the Device Package before the phone firmware upgrade may render the phones unusable.

Features Available with the Firmware Release

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

Client Matter Code and Forced Authorization Code

You can configure the conference phone so that users must enter a billing code or authorization code (or both codes) after they dial a phone number. The billing code, called a Client Matter Code, is used for accounting or billing purposes. The authorization code, called a Forced Authorization Code, controls access to certain phone numbers.

When both a billing code and an authorization code are configured, users are first prompted for the authorization code and then the billing code.

You set up the access codes in the Cisco Unified Communications Manager. For more information, see the Cisco Unified Communications Manager documentation.

Where to Find More Information

- *Cisco IP Conference Phone 7832 User Guide*

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

Mobile and Remote Access Through Expressway

You can set up Mobile and Remote Access through Expressway (MRA). MRA provides a way for remote workers to easily and securely connect into the corporate network without using a virtual private network (VPN) client tunnel. The feature uses Transport Layer Security (TLS) to secure the network traffic.

You need these to provide MRA to your users:

- Cisco Unified Communications Manager Release 10.5(2) and later
- Cisco Expressway Release 8.7 and later

Where to Find More Information

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

Transport Layer Security Enhancements

Administrators now have improved security over phones that act as a HTTPs server. With the parameter Disable TLS1.0 and TLS1.1 for web access, you can apply TLS1.0, TLS1.1, and TLS 1.2 mode, or just TLS 1.2 mode to any phone, or group of phones that function as a HTTPs server.

For other configurations, TLS protocols are configured on the Cisco Unified Communications Manager. As of Cisco Unified Communications Manager 12.0, there are also TLS settings that are configured by a CLI command. See *Release Notes for Cisco Unified Communications Manager and IM & Presence Service, Release 12.0(1)* for information about new CLI commands on Cisco Unified Communications Manager.

Disable TLS1.0 and TLS1.1 for web access is configured from the Product Specific Configuration Layout pane of your Cisco Unified Communications Manager. Install the latest device package for this feature to function.

Disable TLS1.0 and TLS1.1 is supported on Cisco Unified Communications Manager 11.5(1)SU3 and later.

Where to Find More Information

- *Cisco IP Phone 7832 Series 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 Firmware Release 12.1(1) 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.

-
- 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 **12.1(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.12-1-1-12.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-7832.12-1-1-12.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.

-
- 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 **12.1(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 *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 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.

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

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=284883944&rls=12.1\(1\),12.1\(1.*\)&sb=anfr&svr=3nH&bt=custV](https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=284883944&rls=12.1(1),12.1(1.*)&sb=anfr&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=284883944&rls=12.1\(1\)&sb=af&sts=open&svr=3nH&bt=custV](https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=284883944&rls=12.1(1)&sb=af&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=284883944&rls=12.1\(1\),12.1\(1.*\)&sb=fr&sts=fd&svr=3nH&bt=custV](https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=284883944&rls=12.1(1),12.1(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

The following list contains the severity 1, 2, and 3 defects that are open for the Cisco IP Conference Phone 7832 that uses Firmware Release 12.1(1).

For more information about an individual defect, you can access the online record for the defect from the Bug Search Toolkit. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, the list reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects or to view specific bugs, access the Bug Search Toolkit as described in [View Caveats, on page 6](#).

- CSCvi33608: Unable to add phone number to PD entry if no numbers before

Resolved Caveats

The following list contains the severity 1, 2, and 3 defects that are resolved for the Cisco IP Conference Phone 7832 that uses Firmware Release 12.1(1).

For more information about an individual defect, you can access the online record for the defect from the Bug Search Toolkit. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, the list reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of resolved defects or to view specific bugs, access the Bug Search Toolkit as described in [View Caveats, on page 6](#).

- CSCvf29961: menu index is cut in display
- CSCvf37246: phone cannot return to idle page,when decline the speed dial
- CSCvf38731: when failover to srst ,Some softkeys lost
- CSCvf38923: the phone UI don't change to remote in use status
- CSCvf40608: "conf" softkey shows up when ignore the incoming call toast on SRST
- CSCvf50814: Text: "problem loading the ringtone" can't be full displayed
- CSCvf53427: Active server and Stand-by-Server display abnormality at information when config security profile
- CSCvf55233: Dial an invaild number will lost the lock flag when config security profile
- CSCvf64028: Phone should use "System Information" instead of "Phone Information"
- CSCvf79669: Phone should not play the EnergyWise audible alert and display power off message when it power on
- CSCvg61391: add Select softkey for 78xx MRA and input-method switch softkey for Service Domain input
- CSCvg65740: have a toast "Reg Send Failure : REGISTER" when registering
- CSCvh27112: DUT stuck after login, logout EM and Callback function

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 `ciscoem.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 <http://www.cisco.com/c/en/us/support/docs/collaboration-endpoints/unified-ip-phone-7900-series/116684-technote-ipphone-00.html>.

Documentation, Service Requests, and Additional Information

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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.

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/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)

© 2018 Cisco Systems, Inc. All rights reserved.