Cisco IP Conference Phone 8832 Release Notes for Firmware Release 12.1(1)

First Published: 2018-05-14

Cisco IP Conference Phone 8832 Release Notes for Firmware Release 12.1(1)

These release notes support the Cisco IP Conference Phone 8832 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
8832	SIP	Cisco Unified Communications Manager 10.5(2) and later Cisco Unified Communications Manager time zone update 2016d 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 8832 Documentation

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

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/tsd-products-support-general-information.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 Cisco IP Conference Phone 8832 phone so that users must enter a billing code, or authorization code, or both codes after they dial a phone number. The billing code is called a Client Matter Code and 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 *Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*.

Where to Find More Information

- *Cisco IP Conference Phone 8832 User Guide*

Daisy Chain Support

Daisy chain mode enables you to use two or more phones together for improved audio coverage. This configuration is ideal for larger conference rooms or a meeting with numerous people present.

In daisy chain mode, both units receive power though the Smart Adapter which is connected to a power adapter. You can use only one microphone per unit. You can use the units with either a pair of wired or wireless microphones, but you cannot use both microphones together.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Administration Guide for Cisco Unified Communications Manager*
- *Cisco IP Conference Phone 8832 User Guide*

G.722.2 AMR-WB Support

The Cisco IP Conference Phone 8832 now supports the G.722.2 Adaptive Multirate Wideband (AMR-WB) audio codec. This codec offers improved audio, a lower bit-rate compression, and enhanced network performance during peak traffic time.

Where to Find More Information

Cisco IP Conference Phone 8832 Series Administration Guide for Cisco Unified Communications Manager

Wireless Microphone Support

The Cisco IP Conference Phone 8832 supports up to two optional, wireless expansion microphones. Wireless microphones are ideal for large meetings or conference rooms where people are separated from the phone, but still wish to participate in the call.

The wireless expansion microphone kit includes the microphones and a charging cradle.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Administration Guide for Cisco Unified Communications Manager*
- *Cisco IP Conference Phone 8832 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

The Cisco IP Conference Phone 8832 now supports Mobile and Remote Access through Expressway (MRA). MRA allows 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 the following 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 8832 Administration Guide for Cisco Unified Communications Manager*
- *Cisco IP Conference Phone 8832 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 enabled, you can only apply TLS1.2 mode, or you can apply TLS1.0, TLS1.1 and TLS1.2 mode to any phones, 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 8832 Series Administration Guide for Cisco Unified Communications Manager*

Wi-Fi Support and Wireless LAN Profiles

The Cisco IP Conference Phone 8832 now supports Wi-Fi for improvement mobility and a more flexible deployment.

You can use Wireless LAN profiles to enable users to easily access the Wi-Fi network without more configuration. This helps you control network access while you make it easier for users to access your network. You can download and apply one profile to a phone.

To configure a Wireless LAN profile on Cisco Unified Communication Manager, navigate to Cisco Unified Communications Administration and select **Device** > **Device Settings** > **Wireless LAN profile**.

You can apply a Wireless LAN profile to just one phone or to a group of phones. But you can configure only one Wireless LAN profile per group. If the authentication mode of the Wireless LAN profile group is None, then the existing configured profile is removed.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Administration Guide for Cisco Unified Communications Manager*
- *Cisco IP Conference Phone 8832 User Guide*

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, reboot all the servers.

Warning The Cisco IP Conference Phone 8832 PoE Injector is supported on phones running firmware release 12.0(1)SR2 and later. Confirm that the latest firmware release is installed on the Cisco Unified Communications Manager before you connect the Cisco IP Conference Phone 8832 with the PoE injector to the network.

If you are not using the latest firmware release, then your phone may downgrade to an earlier firmware release, and lose network connectivity.

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.

Procedure

Step 1 Go to the following URL:

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

Step 2 Choose **IP Conference Phone 8832**.

Step 3 Choose **Session Initiation Protocol (SIP) Software**.

Step 4 In the Latest Releases folder, choose **12.1(1)**.

Step 5 Select the firmware file, click the **Download** or **Add to cart** button, and follow the prompts.

The firmware filename is cmterm-8832-sip.12-1-1-23.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 6 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 7 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-8832.12-1-1-23.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 **IP Conference Phone 8832**.

Step 3 Choose **Session Initiation Protocol (SIP) Software**.

Step 4 In the Latest Releases folder, choose **12.1(1)**.

Step 5 Download the relevant zip files.

Step 6 Unzip the files.

Step 7 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 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

Firmware Limitation of Cisco IP Conference Phone 8832 with Cisco IP Conference Phone 8832 PoE Injector

The Cisco IP Conference Phone 8832 PoE Injector is supported on phones running firmware release 12.0(1)SR2 and later. Confirm that the latest firmware release is installed on the Cisco Unified Communications Manager before you connect the Cisco IP Conference Phone 8832 with the PoE injector to the network.

If you are not using the latest firmware release, then your phone may downgrade to an earlier firmware release, and lose the network connectivity.

To recover a phone that has lost network connectivity, update Device Defaults for the Cisco IP Conference Phone 8832 to **8832-sip.12-0-1SR2-2.k3.cop.sgn** or later in Cisco Unified Communications Manager Administration. Then, perform one of the following steps:

- Force the phone to reboot from the alternate software image that supports the PoE Injector. To reboot your phone from the backup image, see **Boot Up the Conference Phone from the Alternate Partition** section in the *Cisco IP Conference Phone 8832 Administration Guide for Cisco Unified Communications Manager*.
- Install and use the Cisco IP Conference Phone 8832 Ethernet Injector on the phone. This allows you to regain network connectivity. After the phone has upgraded to the latest firmware, you can again use the Cisco IP Conference Phone 8832 PoE Injector.

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**.

Wireless Microphone Battery Limitation

When you press the **Show detail** softkey, the Cisco IP Conference Phone 8832 occasionally displays a false `Bad battery` warning. This issue occurs when you quickly reseat the wireless microphone 20 consecutive times or more.

To recover from this issue, perform the following steps in order:

- Remove the microphone from the charging cradle.
- Press the Mute button for approximately 10 seconds or until the microphone LED stops blinking white. Then, reseat the microphone on the charging cradle.
- Restart the phone by disconnecting and reconnecting the Cisco IP Conference Phone 8832 Power Adapter.

  The `Bad battery` warning on the phone screen disappears and the current battery status appears. If you do not see the battery status, then the microphone battery has deteriorated and you must replace it.

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=284729655&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=284729655&rls=12.1(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=284729655&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 8832 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 7.

- CSCvg04665: Keep in connecting status while 802.11 mode error
- CSCvg82800: WIFI list and security mode shows wrong about CCKM+WPA2+AES
- CSCvg99422: Audio path is connected before secondary phone is synced
- CSCvh27756: 8832 with smart adapter can not link up after switch changes speed from 10 to 100
- CSCvh46147: The "Network statistics" show "No link" when configure the switch port with same settings "100half"
- CSCvh61133: RTCP always open twice when call connected
- CSCvh78712: wireless mic takes about 2s to setup media
- CSCvi19720: One way audio is heard at the far end of 8832 phone when near and far end user yell at the same time
- CSCvi98837: 8832 can connect the ssid while 802.11 mode error
- CSCvj01727: 8832 cannot change 802.11 mode from 2.4G to 5G after fail to connect with ssid by other softkey
- CSCvj03598: 8832 cannot set static IP manully on wifi (without default router)

Resolved Caveats

The following list contains the severity 1, 2, and 3 defects that are resolved for the Cisco IP Conference Phone 8832 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 7.

- CSCvf26273: when reset on cucm ,phone will only display Settings
- CSCvf29812: XSI service menu item with 64-character long
- CSCvf31609: Port 6970 is always listening after downloading invalid load

- CSCvf33608: EM logout ,phone will flash a "Feature is unavilable “
- CSCvf33885: Scroll bar doesn't disappear when call back
- CSCvf35331: IPv6 setup's UI is not consistent with UI spec
- CSCvf36971: Press "Swap" rapidly will enter "calls" ,when have two speed dial calls.
- CSCvf71182: Recent shows wrong softkey page when accessed from off hook dial
- CSCvf71327: 8832 with IPv6 mode failed to upgrade via TFTP
- CSCvf73723: domain name should be able to be editted even only ipv4 or ipv6 is disabled.
- CSCvf76301: Long Caller ID overlaps the "remote" when in remote in use state
- CSCvg08330: Mute icon display bit slow
- CSCvg26734: Security alerts for curl component of 8832 on October, 2017
- CSCvg39608: eee is not working as expected
- CSCvg47575: 8832 drops some packets when doing image upgrade via http.
- CSCvg47601: 832 doesn't send CDP as first frame when phone boots up (ethernet adapter).
- CSCvg77548: 8832 drop unicast 802.1x packets in the 802.1x Multi-domain situation(ethernet adapter).

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.

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.