Cisco Webex Wireless Phone 800 Series Release Notes for Firmware Release 1.1(0)

First Published: 2021-01-08

Cisco Webex Wireless Phone 800 Series Release Notes for Software Release 1.1(0)

These release notes support the Cisco Webex Wireless Phone 800 Series software release 1.1(0). These wireless smartphones require:

- Cisco Unified Communications Manager (Unified CM):
  - Minimum: 11.5(1)
  - Recommended: 12.5(1) or higher
- Supported Wi-Fi access point.

  See the *Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide* for supported access point options.

Features

Like other devices powered by Android, your phone is app-driven and includes several different Cisco apps that provide various features and functionality.

- Call control:
  - Place and receive phone calls.
  - Put calls on hold.
  - Transfer calls.
  - Have conference calls.
  - Forward calls.
- Monitor the phone battery life.
- Customize the phone buttons.
- If configured, provide emergency safety features such as alarms and motion monitoring.
- If configured, send group broadcasts.
- For the 800S phones, scan barcodes.

Related Documentation

Use the following sections to obtain related information.

Cisco Webex Wireless Phone 800 Series Documentation

Find documentation specific to your phone model and language on the product support page for the Cisco Webex Wireless Phone. From this page, you can also find the Deployment Guide.

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

Installation

Download COP Files for Cisco Unified Communications Manager

Download the following two Cisco Webex Wireless Phone 860 Cisco Options Package (COP) files to install on all Cisco Unified Communications Manager servers in the cluster.

- Installer file: 1.1(0): cmterm-860-installer.1-1-0.k3.cop.sgn
- Software file: 1.1(0): cmterm-860-sip.1-1-0-881-26148.k3.cop.sgn

Procedure

Step 1 Go to the following URL:

https://software.cisco.com/download/home/286327931

Step 2 Choose **Webex Wireless Phone**.

Step 3 Choose **Webex Wireless Phone 860**.

Step 4 In the **Latest Releases** folder, choose **QED Installer**, select the installer file, click the **Download** or **Add to cart** button, and follow the prompts.

- Installer file: cmterm-860-installer.1-1-0.k3.cop.sgn

Step 5 In the **Latest Releases** folder, choose **1.1(0)**, select the software file, click the **Download** or **Add to cart** button, and follow the prompts.

- Software file: cmterm-860-sip.1-1-0-881-26148.k3.cop.sgn

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

Step 6 Click the + next to the software filename in the Download Cart section to access additional information about this file.

Note The hyperlink for the readme file is in the Additional Information section.

Load the COP Files to Cisco Unified Communications Manager

You must install the Cisco Webex Wireless Phone 800 Series device enabler QED installer and phone software Cisco Options Package (COP) files into each Cisco Unified Communications Manager (Unified Communications Manager) in the cluster.

Note These COP files are signed with the sha512 checksum. Cisco Unified Communications Manager versions before version 14 don't automatically include support for sha512.

For the first installation, install the device enabler QED installer file first and then the software file.

For future software updates, there is not always a corresponding device enabler QED installer update. When a software update is available, check the latest version of the device enabler QED installer file to see whether you also must update it.

Before you begin

- Download the device enabler QED installer and phone software COP files from the software download site:

  https://software.cisco.com/download/home/286327931

- If you have Unified Communications Manager version 11.5 or 12.5 and don't already have sha512 checksum support enabled, install ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn.

Caution Choose an appropriate time to perform this task. As part of this task you must restart each Unified Communications Manager in the cluster after you install a device enabler QED installer COP file, unless your version of Unified Communications Manager offers an alternate process that does not require a reboot.

See the *Manage Device Firmware* section of the *Administration Guide for Cisco Unified Communications Manager* for your Unified Communications Manager version, to see if it allows an installation process that does not require a reboot.

Procedure

Step 1 In each Unified Communications Manager in the cluster, select **Cisco Unified OS Administration** > **Software Upgrades** > **Install/Upgrade**.

Step 2 Enter the Software Location data.

Step 3 Click **Next**.

Step 4 Select the COP (.cop.sha512) file.

Note If the COP file doesn't appear in the available files list, ensure that you enable sha512 checksum support.

Step 5 Click **Next** to download the COP file to Unified Communications Manager.

Step 6 Check that the file checksum details are correct.

Step 7 Click **Next** to install the COP file on Unified Communications Manager.

Step 8 Click **Install Another** and repeat steps 2–7 to install another COP file.

Step 9 Perform the following actions based on the COP files that you installed.

a) If you installed a device enabler QED installer COP file:

- **For 11.5(1)SU4 and lower**:
  - Reboot all Unified Communications Manager nodes through **Cisco Unified OS Administration** > **Settings** > **Version** > **Restart**.
- **For 11.5(1)SU5 and higher or 12.5(1) and higher**:
  - Restart the Cisco Tomcat service on all Unified Communications Manager nodes.
  - If running the Unified Communications Manager service on the publisher node, restart the service on the publisher node only. You do not need to restart the Cisco Call Manager Service on subscriber nodes.

b) If you installed a software COP file, restart the Cisco TFTP service for all nodes running the Cisco TFTP service.

Install Manufacturing CA Certificates

The phones use a new manufacturing certificate authority (CA). Until Cisco Unified Communications Manager (Unified Communications Manager) includes these new certificates, you must manually add the new root and intermediate certificates to the certificate chain to trust the new Manufacturing Installed Certificates (MIC). After you add the new certificates to the trust chain, the MICs can be used for trust services such as SIP TLS, Configuration File Encryption, and LSC Certificate distribution.

Procedure

Step 1 Download the missing root and intermediate certificates from the externally available Cisco PKI website. The missing certificates to complete the trust chain up to and including the root for the new MICs are:

- Cisco Manufacturing CA III (cmca3) - Intermediate
- Cisco Basic Assurance Root CA 2099 (cbarc2099) - Root for Cisco Manufacturing CA III

Step 2 From your web browser, log in to the **Cisco Unified Operating System Administration** web page.

Step 3 Under the **Security** menu, select **Certificate Management**.

Step 4 Select **Upload Certificate/Certificate Chain**.

Step 5 Select **CallManager-trust** for the **Certificate Purpose**, browse to the certificate, then select **Upload**.

Repeat this step for all certificates on the Unified Communications Manager Publisher only as the certificate replicates to all other Unified Communications Manager nodes.

Step 6 Select **CAPF-trust** for the Certificate Purpose, browse to the certificate, then select **Upload**.

Repeat this step for all certificates on all Unified Communications Manager nodes as the certificate will not replicate to all other Unified Communications Manager nodes automatically.

Limitations and Restrictions

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=286327931&rls=1.1%280%29&sb=anfr&bt=custV

- Use this URL for all open caveats:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286327931&rls=1.1%280%29&sb=afr&bt=custV

- Use this URL for all resolved caveats:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286327931&rls=1.1%280%29&sb=fr&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

The following list contains the severity 1, 2, and 3 defects that are open for the Cisco Webex Wireless Phone 800 Series software release 1.1(0).

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 5.

- CSCvv86452 EAP method cannot change from PEAP to TTLS on a saved network
- CSCvv86446 CP-860 wifi can't scan the ap with channel 12 or channel 13
- CSCvw50733 New Wi-Fi network parameters do not show after editing a Wi-Fi network if remain in Wi-Fi details
- CSCvw13004 CP860 Fast roaming with CCKM failed
- CSCvw37475 Voicemail tab remains visible in Cisco Phone app if Visual Voicemail is Enabled then Disabled later
- CSCvv88242 Phone doesn't refresh the network edit page after changing the security mode when SSID is connected
- CSCvw54482 Phone does not look at the Block Caller-ID setting in the SIP profile
- CSCvw25957 Phone unregisters after Wi-Fi disconnect / session timeout
- CSCvw30089 CP860 can not remember the wifi SSID last time used
- CSCvw50748 CA Certificate config resets to "Please select" when editing a saved EAP enabled Wi-Fi network
- CSCvv92095 There will have overlap when view phone trusted credentials
- CSCvw24021 In Add network page "cancel /save“ overlap the configure page
- CSCvw24841 CAPF stuck in pending state

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)