# Cisco Webex Wireless Phone 800 Series Release Notes for Firmware Release 1.2(0)

**First Published:** 2021-03-29

# Cisco Webex Wireless Phone 800 Series Release Notes for Firmware Release 1.2(0)

These release notes support the Cisco Webex Wireless Phone 800 Series software release 1.2(0). These wireless smartphones require:

- Cisco Unified Communications Manager (Unified Communications Manager):
  - 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.

## New and Changed Features

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

### DHCP Option 66 Support

In addition to DHCP option 150, this release also supports DHCP option 66. DHCP option 66 autoconfigures the Cisco Unified Communications Manager server address. It is in ASCII format, not IP address format and supports a single server name.

#### Where to Find More Information

*Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide*

*Cisco Webex Wireless Phone 800 Series Administration Guide for Cisco Unified Communications Manager*

### Sounds Settings in the Custom Settings App

The **Sounds** settings allow you to set which sounds are available for the ringtones, notifications, and alarms. You can also change the default sound for each.

#### Where to Find More Information

*Cisco Webex Wireless Phone 800 Series Administration Guide for Cisco Unified Communications Manager*

### Advanced Data Formatting in ScanFlex

The **Advanced Data Formatting** settings allow you to select barcode symbologies and set custom actions for a ScanFlex application.

#### Where to Find More Information

*Cisco Webex Wireless Phone 800 Series Administration Guide for Cisco Unified Communications Manager*

## Related Documentation

Use the following sections to obtain related information.

### Cisco Webex Wireless Phone 800 Series 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/webex-wireless-phone/series.html

Locate the Deployment Guide at the following URL:

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/800-series/deployment/840_860_wlandg.pdf

### 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 correct device enabler (QED) installer and software Cisco Options Package (COP) files for your phone and Cisco Unified Communications Manager (Unified Communications Manager) version, so that you can install them on the Unified Communications Manager servers in the cluster.

#### Procedure

**Step 1** Go to the following URL:

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

**Step 2** From **Webex Wireless Phone**, choose the phone model.

**Step 3** Choose **Latest Releases** > **QED Installer**, and then click either **Download** or **Add to Cart** for the required installer COP file.

**Device Enabler QED Installer COP files for 840**:

- For Unified Communications Manager 11.5 and 12.5: cmterm-840-installer.1-2-0.k3.cop.sgn
- For Unified Communications Manager 14: cmterm-840-installer.1-2-0.k3.cop.sha512

**Device Enabler QED Installer COP files for 860**:

- For Unified Communications Manager 11.5 and 12.5: cmterm-860-installer.1-1-0.k3.cop.sgn

  **Note** There is no update to the device enabler (QED) installer COP file for Cisco Webex Wireless Phone 860 specific to the 1.2.0 software release. If you've already enabled your 860 devices with the 1.1.0 device enabler COP file, you don't need to update the device enabler COP file.

- For Unified Communications Manager 14: Unified Communications Manager 14 automatically includes the 1.1.0 version of the device enabler support files for the 860 devices, so you don't need to download or install a separate device enabler COP file.

**Note** To access more details about the COP files, such as the Checksum details and a link to the **Readme** file, hover the mouse pointer over the filename.

**Note** If you chose to click **Download**, follow the prompts.

**Step 4** Choose **Latest Releases** > **1.2(0)**, and then click either the **Download** or **Add to Cart** button for the required software COP file.

**Software COP files for 840**:

- For Unified Communications Manager 11.5 and 12.5: cmterm-840-sip.1-2-0-658-27763.k3.cop.sgn
- For Unified Communications Manager 14: cmterm-840-sip.1-2-0-658-27763.k3.cop.sha512

**Software COP files for 860**:

- For Unified Communications Manager 11.5 and 12.5: cmterm-860-sip.1-2-0-1003-27763.k3.cop.sgn
- For Unified Communications Manager 14: cmterm-860-sip.1-2-0-1003-27763.k3.cop.sha512

**Note** If you chose to download the file, follow the prompts.

If you chose to add the files to your cart, click the **Cart** when you are ready to download all the files.

## Load the COP Files to Cisco Unified Communications Manager

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

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

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

**Note** With each new software release, the Cisco apps are also updated in the Play Store. However, if you manage the phones through an Enterprise Mobility Management (EMM) application, we recommend that you update the firmware on the phones to minimize any risk of app incompatibility.

### Before you begin

Download the installer and phone software COP files from the software download site:

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

**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 an 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.sgn or .cop.sha512) file.

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

**Step 6** Check that the file checksum details look 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 an 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.

# Caveats

## View Bugs

You can search for bugs using the Cisco Bug Search Tool.

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

For more information about how to use the Bug Search Tool, see Bug Search Tool Help.

### Before you begin

To view bugs, 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 view bugs for the 1.2(0) release of the Cisco Webex Wireless Phone 800 Series:

- Use this URL to view all bugs:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286327931&rls=1.2%280%29&sb=anfr&bt=custV

- Use this URL to view all open bugs:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286327931&rls=1.2%280%29&sb=afr&bt=custV

- Use this URL to view all resolved bugs:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286327931&rls=1.2%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 Bugs

The following list contains a snapshot of severity 1, 2, and 3 bugs that were open at the time of the Cisco Webex Wireless Phone 800 Series software release 1.2(0).

For an updated view of open bugs or to view more information about specific bugs, access the Bug Search Tool as described in View Bugs, on page 5.

- CSCvv86446 Unable to connect to an AP on channel 12 or 13 if another AP is not available on channel 1-11
- CSCvw13004 Delayed ARP response from default gateway can cause CP-860 to disconnect when using CCKM
- CSCvw24841 Phone might get stuck in pending state when install LSC
- CSCvw25957 Phone unregisters after Wi-Fi disconnect / session timeout
- CSCvx41815 DN remains displayed in the phone app even when unregistered
- CSCvx49380 XML tag for QED multi-level option "Voicemail Server (Backup)" is incorrect
- CSCvx49473 Password for QED option "Secondary SIP Password" is not masked when entered in CUCM UI

## Resolved Bugs

The following list contains a snapshot of severity 1, 2, and 3 bugs that were resolved at the time of the Cisco Webex Wireless Phone 800 Series software release 1.2(0).

For an updated view of resolved bugs or to view more information about specific bugs, access the Bug Search Tool as described in View Bugs, on page 5.

- CSCvv92095 There is overlap when viewing phone trusted credentials
- CSCvw24021 In Add network page Cancel and Save overlap the configuration page

- CSCvw37475 Voicemail tab remains visible in Cisco Phone app if Visual Voicemail is Enabled then Disabled later
- CSCvw54482 Phone does not look at the Block Caller-ID setting in the SIP profile
- CSCvx29195 CP-860 makes a crackling noise when playing a game
- CSCvx60769 Cisco Phone Android app in continuous registration loop due to config mis-match
- CSCvx60965 OTA download status incorrect when not using load server or CUCM version w/o range header support
- CSCvx61124 In some occasions, Cisco Phone application does not present Waits and Pauses in dial string
- CSCvx63333 Directory Search does not work when phone fails over to secondary server
- CSCvx63343 Phone reboots occasionally after CUCM or user initiates request for prt-report

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)