Webex Wireless Phone 840 and 860 Release Notes for Firmware Release 1.3(0)

First Published: 2021-06-29

Last Modified: 2021-10-20

Cisco Webex Wireless Phone 800 Series Release Notes for Firmware Release 1.3(0)

These release notes support the Webex Wireless Phone 840 and 860 software release 1.3(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 Information

As of October 11, 2021, there is a new 1.3(1) device enabler QED installer file for the 860 phones. We recommend that you use the 1.3(1) file, rather than the original 1.3(0) file. For more details about how to download and install the new device enabler QED installer file for the 860 phones, see Download the COP Files for Release 1.3(0), on page 4.

New and Changed Features

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

Note These features require the latest device enabler QED installer and software COP files.

Multiple Lines

The multiple lines feature allows you to configure up to six lines on a phone. Each phone line has a distinctly numbered and colored circle that is associated with it. Users can make and receive calls from all lines. If you configure the phone to allow multiple calls at once, users can have up to four calls per line at once.

Where to Find More Information

Cisco Webex Wireless Phone 800 Series User Guide

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

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide

System Configuration Guide for Cisco Unified Communications Manager

Cisco Extension Mobility

Cisco Extension Mobility allows different users to use the same phone at different times. This feature allows shift workers to share a single phone. When a user logs in to the phone, it uses their profile configuration including their line numbers, speed dials, and privacy settings. When the user logs out, it removes the user's settings, and applies the default phone configuration.

Where to Find More Information

Cisco Webex Wireless Phone 800 Series User Guide

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

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide

Feature Configuration Guide for Cisco Unified Communications Manager

Shared Lines

The shared line feature allows you to configure the same phone number on more than one phone. When someone calls a shared line, all the phones with that shared line ring, and any user with the shared line can answer the call.

Where to Find More Information

Cisco Webex Wireless Phone 800 Series User Guide

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

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide

Feature Configuration Guide for Cisco Unified Communications Manager

Privacy on Shared Lines

You can enable the privacy feature for shared lines on your phone. When you answer a call with the privacy feature enabled, your coworkers who share the line can't join the call, or see who is on the call. The administrator can enable or disable the privacy feature for each phone or for all phones in a cluster.

You can also enable a limited privacy setting so that your coworkers on your shared line can't pick up a call that you place on hold.

Where to Find More Information

Cisco Webex Wireless Phone 800 Series User Guide

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

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide

Feature Configuration Guide for Cisco Unified Communications Manager

Auto Answer

The auto answer feature allows you to set a phone to automatically connect to incoming calls after a ring or two.

Where to Find More Information

Cisco Webex Wireless Phone 800 Series User Guide

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

Feature Configuration Guide for Cisco Unified Communications Manager

Line Text Label

The line text label feature allows users to set a text label for a phone line instead of using the directory number.

Where to Find More Information

Cisco Webex Wireless Phone 800 Series User Guide

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

Feature Configuration Guide for Cisco Unified Communications Manager

Call Admission Control and Traffic Specification

The administrator can enable Call Admission Control (CAC) and Traffic Specification (TSPEC) for call control and voice on the WLAN controller or access point.

Where to Find More Information

Cisco Webex Wireless Phone 840 and 860 Wireless LAN Deployment Guide

PTT Broadcast on a Locked Phone

The administrator can now set the phones to allow PTT transmissions on a locked phone.

Where to Find More Information

Cisco Webex Wireless Phone 800 Series User Guide

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

Dark Theme and Nearby Share Quick Settings Tiles

If the administrator enables them, users can access these new quick settings tiles:

- **Dark theme**—Changes the display to light text on a dark background.
- **Nearby share**—Enables users to share files, links, and pictures with other devices within a certain range.

Where to Find More Information

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

Custom Settings App Includes Display Settings

The administrator can control the phone's display settings through the Custom Settings app.

Where to Find More Information

Cisco Webex Wireless Phone 800 Series User Guide

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

Related Documentation

Use the following sections to obtain related information.

Webex Wireless Phone 840 and 860 Documentation

Find documentation specific to your phone model and language on the product support page for the 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 on the product support page.

Installation

Download the COP Files for Release 1.3(0)

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

Device Enabler QED Installer COP file for 840: cmterm-840-installer.1-3-0.k4.cop.sha512

Device Enabler QED Installer COP file for 860: cmterm-860-installer.1-3-1.k4.cop.sha512

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** > **1.3(0)**, and then click either the **Download** or **Add to Cart** button for the required software COP file.

Software COP file for 840: cmterm-840-sip.1-3-0-818-30905.k4.cop.sha512

Software COP file for 860: cmterm-860-sip.1-3-0-1135-30905.k4.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 Webex Wireless Phone 840 and 860 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.

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 device enabler QED installer and phone software COP files from the Software Download site.
- 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

Largest Font Size

If you set the font size to **Largest** in the phone **Settings**, it may cut off some text. For example, if you set the phone to call forward, it may cut off the lower part of the display text that shows where the calls are forwarded.

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 1.3(0) release of the Webex Wireless Phone 840 and 860:

- View all bugs.

- View all open bugs.
- View all resolved bugs.

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 a snapshot of severity 1, 2, and 3 bugs that were open at the time of the Webex Wireless Phone 840 and 860 software release 1.3(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 7.

- CSCvw13004 Delayed ARP response from default gateway can cause CP-860 to disconnect when using CCKM
- CSCvx62886 Multiple Vulnerabilities in Frame Aggregation and Fragmentation Implementation of 802.11
- CSCvy30608 840 move from same SSID with different VLAN interface, 840’s ip addr not change.
- CSCvy47178 Remote side in call preservation mode after 860 roaming from AP1 to AP2 with CCKM enabled.
- CSCvy50683 840 send disassociate to AP2 with reason code:0x0001 during FT roaming
- CSCvy51577 840 do full EAP authentication during fast roaming with CCKM
- CSCvy54731 840 can't auto re-connected to the SSID after change some parameters of this SSID on WLC
- CSCvy54880 Sometimes interband roaming failed.
- CSCvy59852 No DN displayed on Incoming alert UI when display name config
- CSCvy59855 UI error when config 24 digit DN as share line number
- CSCvy59858 UI error while CFW with 'Caller Name'&'Caller Number'&'Redirected Number'&'Dialed Number' enabled
- CSCvy81870 Webex 840 doesn't display secure lock icon for encrypted call when answering within native phone app
- CSCvy85323 Some values for Panic Button option when managing the Emergency app via an EMM are not working

Resolved Caveats

The following list contains a snapshot of severity 1, 2, and 3 bugs that were resolved at the time of the Webex Wireless Phone 840 and 860 software release 1.3(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 7.

- 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
- CSCvx84322 Evaluation of 860-840-family for OpenSSL March 2021 vulnerabilities
- CSCvy02033 840 phone sends ps poll to retrieve buffered frames when it should send a trigger frame
- CSCvy04502 Web Access in Web API app does not re-sync with CUCM Web Access config if Web API was changed
- CSCvy06327 The phone Web Password is cached and still used even if cleared in CUCM and the phone is reset
- CSCvy27764 860 can't connected to PSK SSID with adaptive 11r enabled