Cisco Wireless Phone 840 and 860 Release Notes for Firmware Release 1.6(0)

First Published: 2022-06-29

Last Modified: 2022-07-26

Cisco Wireless Phone 840 and 860 Release Notes for Firmware Release 1.6(0)

These release notes support the Cisco Wireless Phone 840 and 860 software release 1.6(0). These wireless smartphones require:

- Cisco Unified Communications Manager (Unified Communications Manager):
  - Minimum: 11.5(1)
  - Recommended: 12.5(1), 14.0(1), or higher
- Supported Wi-Fi access point.

  See the Cisco Wireless Phone 840 and 860 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.

Webex Calling support

Webex Calling is now supported for Cisco Wireless Phone 840 and 860.

For more information on Webex Calling, see: https://help.webex.com/ld-nzid8xi

Generate problem reports through the Cisco Wireless Phone webpage

Problem reports can now be generated from the Cisco Wireless Phone 840 and 860 webpage.

Capture network traces through the Cisco Wireless Phone webpage

Network traces can now be captured from the Cisco Wireless Phone 840 and 860 webpage.

Firmware upgrade tool

Cisco Wireless Phone Upgrade Tool @https://webexphoneupgrade.cisco.com allows users to upgrade the firmware from all the previous releases to the current release 1.6.0 which enables Webex Calling support.

Related Documentation

Use the following sections to obtain related information.

Cisco Wireless Phone 840 and 860 documentation

Find documentation specific to your phone model and language on the product support page for the Cisco Wireless Phone. From this page, you can also find the Cisco Wireless Phone 840 and 860 Deployment Guidee.

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 1.6(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 Software Download page for the phones.

Step 2 From **Cisco 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.1-5-0.k4.cop.sha512

Device Enabler QED Installer COP file for 860: cmterm-860-installer.1-5-0.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** > **1.6(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.1-6-0-1409-48122.k4.cop.sha512

Software COP file for 860: cmterm-860-sip.1-6-0-1852-48122.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 Cisco 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.

Caveats

View Caveats

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 Click the following links to view bugs for the 1.6(0) release of the Cisco Wireless Phone 840 and 860:

- View All Caveats.
- View all Open Caveats.
- View all Resolved Caveats.

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 Cisco Wireless Phone 840 and 860 software release 1.6(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 Caveats.

- CSCwa01438 840/860 logs out of EMCC when the phone is restarted
- CSCwb11302 When using EMMA the EAP Phase 2 auth options for PEAP should only be MSCHAPV2 and GTC
- CSCwc09897 Web access is disabled when the phone is manually put into WxC mode and the profile rule is entered.

- CSCwc31472 WxC: Resync_Periodic not occur at the specific time period

Resolved Caveats

The following list contains a snapshot of severity 1, 2, and 3 bugs that were resolved at the time of the Cisco Wireless Phone 840 and 860 software release 1.6(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 Caveats.

- CSCwb31325 Cisco 860 phone displays the wrong number after transfer