Cisco Wireless IP Phone 8821 and 8821-EX Release Notes for Firmware Release 11.0(6)SR2

First Published: 2021-12-16

Cisco Wireless IP Phone 8821 and 8821-EX Release Notes for Firmware Release 11.0(6)SR2

These release notes support the 11.0(6)SR2 firmware release for the Cisco Wireless IP Phone 8821 and 8821-EX.

The following table describes the supported call control platforms for this release.

Table 1: Call Control Platform

Call Control Platform	Minimum Version	Recommended Versions
Cisco Unified Communications Manager	9.1(2)	11.5, 12.0, 12.5, 14 or later
Cisco Unified Communications Manager Express	10.5	11.7 or later
Cisco Unified Survivable Remote Site Telephony	10.5	11.7 or later

The following table describes the supported wireless access points and versions for this release.

For more details about compatible wireless access points, see the Cisco Wireless IP Phone 8821 and 8821-EX Wireless LAN Deployment Guide.

Table 2: Wireless Access Points

Access Point Hardware	Minimum Version	Recommended Versions
Cisco AireOS Wireless LAN Controller and Cisco Lightweight Access Points	8.0.121.0	8.3.150.0, 8.5.171.0, 8.8.130.0, 8.10.151.0
Cisco Catalyst IOS XE Wireless LAN Controller and Cisco Lightweight Access Points	16.12.1s	16.12.5, 17.3.3, 17.4.1
Cisco Mobility Express and Cisco Lightweight Access Points	8.3.143.0	8.3.150.0, 8.5.171.0, 8.8.130.0, 8.10.151.0

Access Point Hardware	Minimum Version	Recommended Versions
Cisco Autonomous Access Points	12.4(21a)JY	15.2(4)JB6, 15.3(3)JF12i, 15.3(3)JPK
Cisco Meraki Access Points	MR 25.9, MX 13.33	MR 27.6, MX14.53

Related Documentation

Use the following sections to obtain related information.

Cisco Wireless IP Phone 882x Series Documentation

Find documentation that is specific to your phone model, call control system, and language on the product support page for the Cisco Wireless IP Phone 8821 and Cisco Wireless IP Phone 8821-EX. From these pages, you can also find the Cisco Wireless IP Phone 8821 and 8821-EX Wireless LAN 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.

Cisco Unified Communications Manager Express Documentation

See the publications that are specific to your language, phone model, and release on the product support page for Cisco Unified Communications Manager Express.

New and Changed Features

This release contains no new or changed features.

Installation

Installation Requirements

Before you install the firmware release, you must ensure that your Cisco Unified Communications Manager is running the latest device package. After you install a device package on the Cisco Unified Communications Manager servers in the cluster, you need to reboot all the servers.

Note If your Cisco Unified Communications Manager doesn't have the required device package to support this firmware release, the firmware may not work correctly.

For information on the device packages, see the Cisco Unified Communications Manager Device Package Compatibility Matrix.

Install Firmware Release 11.0(6)SR2 on Cisco Unified Communications Manager

Before you can use 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.

Before you begin

The Cisco Options Package (COP) file for this release is signed with the sha512 checksum. Versions of Cisco Unified Communications Manager before version 14 don't have built-in support for sha512, so for those versions, you must first enable sha512 checksum support.

Note If you try to install the sha512 COP file on a Cisco Unified Communications Manager that doesn't support the sha512 checksum, the COP file doesn't appear in the list of available files.

To enable sha512 checksum support, install ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn. For directions on how to install this file, see this release note document.

Procedure

Step 1 Go to the **IP Phone 8800 Series** Software Download page.

Step 2 Click **Wireless IP Phone 8821**.

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

Step 4 From the **Latest Releases** folder, click **11.0(6)SR2**.

Step 5 Click either **Download** or **Add to Cart** next to the firmware file, and follow the prompts.

Firmware file: cmterm-8821-sip.11-0-6SR2-4.k4.cop.sha512

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

Step 6 To access more details about the file, such as the Checksum details and a link to the Readme file, hover the mouse pointer over the filename.

a) Click **Readme** to access the installation instructions for the corresponding firmware.

b) Follow the instructions in the **Readme** file to install the firmware.

Install Firmware Release 11.0(6)SR2 on Cisco Unified Communications Manager Express

Before you can use the phone firmware release on Cisco Unified Communications Manager Express, you must download the firmware image file from the software download center and install it.

For information about Cisco Unified Communications Manager Express support, see the Phone Feature Support Guide for Unified CME, Unified SRST, Unified E-SRST, and Unified Secure SRST.

For more information about this procedure, see the *Install and Upgrade Cisco Unified CME Software* chapter in the Cisco Unified Communications Manager Express System Administrator Guide.

Procedure

Step 1 Go to the **IP Phone 8800 Series** Software Download page.

Step 2 Click **Wireless IP Phone 8821**.

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

Step 4 From the **Latest Releases** folder, click **11.0(6)SR2**.

Step 5 Click **Download** or **Add to Cart** next to the following zip file and follow the prompts.

Zip file: cmterm-8821.11-0-6SR2-4.zip

Step 6 Extract the files from the zip file, manually copy them to the Cisco Unified Communications Manager Express TFTP server (router flash), and enable them for TFTP.

Limitations and Restrictions

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone audio and video quality, and in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

Anything that degrades network performance can affect phone audio 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.

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.

Recording Tone Volume Limitation

If you use the recording feature, we recommend that you change the **Recording Tone Local Volume** configured in Cisco Unified Communications Manager. Change the field from the default of 100 to 20, as described in CSCvc14605.

The Cisco Unified Communications Manager device packs (October 2017 and later) have the default set to 20.

TLS 1.2 Tunnel Limitation with ISE 2.0 to 2.3

To support a TLS 1.2 tunnel between the phone and the Cisco Identity Service Engine (ISE) server, the ISE patch to resolve CSCvm03681 must be applied. This patch is required for ISE servers running Release 2.0 to 2.3; ISE Release 2.4 and later include the patch.

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 Click the following links to view bugs for the 11.0(6)SR2 release of the Cisco Wireless IP Phone 8821 and 8821-EX:

- View all bugs.
- View open bugs.
- View 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 Bugs

The following list contains a snapshot of the severity 1, 2, and 3 bugs that were open at the time of the Cisco Wireless IP Phone 8821 and 8821-EX Firmware Release 11.0(6)SR2.

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 4.

- CSCvh47665 No Secure tone played on protected phones while enable speaker
- CSCvj88754 Failed to Log Out from personal directory
- CSCvm66028 Phone will eventually loose WiFi when roaming between 2 AP's set at 80MHz/40MHz
- CSCvm69293 Network configuration info not displayed on current wlan profile
- CSCvm74978 8821 phone sometimes couldn't receive the EAP identity request on 2.4G JFW test bed.
- CSCvn05182 UI error while enable FAC
- CSCvn18501 MLPP priority lost in session bubble during xfer/conference
- CSCvn58894 8821 Personal Directory Login should not display again after success login & exit without logout
- CSCvn63992 UI: missing SSID if in neighbor list before WLAN connection
- CSCvn81608 Java process sometimes has significant delay in receiving events from wlanmgr after OOR & In Range
- CSCvo05996 No Recording Tone heard after hold/resume several times.

- CSCvo08723 Phone not able to re-connect to highest priority WLAN profile after connect to lower priority one
- CSCvo10371 Phone did not do full authentication after deauth 7 causing call preservation
- CSCvo46442 Phone shut down when battery was showing 13%
- CSCvo74044 Hear short sharp ring tone during hold revert with Chirp1&2 ringtone and RIU session.
- CSCvo74177 Sometimes(90%) ringer is very low in hold reversion state when ringer volume is maximized
- CSCvo82607 Wrong behavior after press red key on originator phone in conference call when failover to SRST
- CSCvp14422 Phone will not roam from 5GHz WLAN profile to 2.4GHz WLAN profile if SSID disabled via WLC
- CSCvr86735 Phone does not ring for hold reverted call after disconnecting another active call
- CSCvs16657 Call is automatically muted when dock station power is disconnected
- CSCvs85963 'undefined' and 'Rcvr packets' swapping on Call statistics screen
- CSCvt02503 Phone no longer plays recording tone after a few calls
- CSCvv04725 8821 has no dial tone after fallback from srst to cucm
- CSCvv45769 8821 can't set local time from LCD if its dhcp server has option 42 configured
- CSCvw29937 8821-EX phone unregistered and didn't register back to CUCM automatically
- CSCvw91213 8821 phone sometimes fails to process the EAP Request packets on 5GHz JFW test bed.
- CSCvw91590 8821 can't make a call when FAC enabled and using Recents list
- CSCvx62510 Cisco IP Phone Cisco Discovery Protocol Out-of-Bound Read Vulnerability
- CSCwa32886 Unable to push a new SSID and PSK via Wireless Device Profiles on CP-8821
- CSCwa43522 After changing the WLAN Profile Group on an 8821, the new additional WLAN Profiles are disabled

Resolved Bugs

The following list contains a snapshot of the severity 1, 2, and 3 bugs that were resolved at the time of the Cisco Wireless IP Phone 8821 and 8821-EX Firmware Release 11.0(6)SR2.

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 4.

- CSCvx16078 Evaluation of IP Phone 8821 for Bluetooth_Pairing_Protocol_2021 vulnerabilities
- CSCvx60095 voice mail doesn't work if visual voice mail configure error
- CSCvx61012 Multiple Vulnerabilities in Frame Aggregation and Fragmentation Implementation of 802.11
- CSCvx63468 Phone can't stop vibrating when end the hold reverted call exceed 10 seconds
- CSCvx82788 Wireless IP Phone 8821 OpenSSL March 2021 vulnerabilities

- CSCvx85821 Cisco IP Phone Software Arbitrary File Read Vulnerability
- CSCvy07843 An invalid channel "0" is added to channel list when doing continuous scan, causing scan failure
- CSCvy67834 Evaluation of sl-wireless-phones for boot script replacement vulnerability
- CSCvy89344 Evaluation of sl-wireless-phones for Bluetooth vulnerability CVE-2020-10370
- CSCvz43035 8821 Phones are not all intiating the re-association request frame to roam
- CSCvz95663 Umlauts letters are shown incorrectly on 8821 WLAN Phones.

Cisco Unified Communication Manager Public Keys

To improve software integrity protection, public keys are used to sign cop files for Cisco Unified Communications Manager Release 10.0.1 and later. These cop files have “k3 or k4” in their name. To install a k3 or k4 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 you must install this additional cop file 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 the Software Download page, 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 the Cisco IP Phone Firmware Support Policy.

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)