



# Cisco Wireless IP Phone 8821 and 8821-EX Release Notes for Firmware Release 11.0(5)SR1

**First Published:** 2019-06-27

**Last Modified:** 2020-08-12

## Cisco Wireless IP Phone 8821 and 8821-EX Release Notes for Firmware Release 11.0(5)SR1

These release notes support the Cisco Wireless IP Phone 8821 and 8821-EX Firmware Release 11.0(5)SR1.

The following table describes the systems and versions that the phone requires.

| System   | Minimum Version         | Recommended Versions                                  |
|--|-------------------------|---|
| Cisco Unified Communications Manager           | 9.1(2)                  | 10.5(2), 11.0(1), 11.5(1), and later                  |
| Cisco Unified Communications Manager Express   | 10.5 through Fast Track | 11.0, 11.5, 11.7 (native support), and later          |
| Cisco Unified Survivable Remote Site Telephony | 10.5                    | 11.0, 11.5, 11.7, and later                           |
| Cisco Wireless LAN Controller                  | 8.0.121.0               | 8.0.152.0, 8.2.170.0, 8.3.143.0, 8.5.140.0, 8.8.120.0 |
| Cisco IOS Access Points (Autonomous)           | 12.4(21a)JY             | 12.4(25d)JA2, 15.2(4)JB6, 15.3(3)JF1                  |
| Cisco Meraki                                   | MR 25.9, MX 13.33       | MR 25.11, MX 13.33                                    |

### Cisco Wireless IP Phone 8821-EX Support

The Cisco Wireless IP Phone 8821-EX is a ruggedized, resilient, and secure 802.11 wireless LAN handset. The phone is designed for use in industrial settings and other places where a phone that is nonsparking and sealed for protection against dust, splash, or water. It is similar to the Cisco Wireless IP Phone 8821, but the phone is yellow to improve visibility, as shown in the following figure.

**Figure 1: Cisco Wireless IP Phone 8821-EX**



The phone has these characteristics that are different from the Cisco Wireless IP Phone 8821:

- IP67 rating
- ATEX Class I, Zone 2 certified
- CSA Class I, Division 2 and Class 1, Zone 2 certified
- MIL-STD-810G tested

You must charge the phone with one of the following chargers:

- Cisco Wireless IP Phone 8821-EX Desktop Charger
- Cisco Wireless IP Phone 8821-EX Multi Charger




---

**Note** The Cisco Wireless IP Phone 8821-EX must use the Cisco Wireless IP Phone 8821-EX Desktop Charger or Cisco Wireless IP Phone 8821-EX Multi Charger for ATEX compliance.

---




---

**Caution** You can't use the chargers designed for the Cisco Wireless IP Phone 8821 to charge the Cisco Wireless IP Phone 8821-EX or its spare batteries.

---

### Where to Find More Information

- *Cisco Wireless IP Phone 8821 and 8821-EX Accessory Guide*
- *Cisco Wireless IP Phone 8821 and 8821-EX Administration Guide*
- *Cisco Wireless IP Phone 8821 and 8821-EX User Guide*

## New and Changed Features

This release contains no new or changed features.

## Related Documentation

Use the following sections to obtain related information.

### Cisco Wireless IP Phone 882x 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/unified-ip-phone-8800-series/tsd-products-support-series-home.html>

The Deployment Guide is located at the following URL:

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html>

### 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>

### Cisco Unified Communications Manager Express Documentation

See the publications that are specific to your language, phone model and Cisco Unified Communications Manager Express release. Navigate from the following documentation URL:

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/tsd-products-support-series-home.html>

## Installation

### Installation Requirements

Before you install the firmware release, you must ensure that your Cisco Unified Communications Manager is running the latest device pack. The applicable device packs are released after the firmware release. After you install a device pack on the Cisco Unified Communications Manager servers in the cluster, you need to reboot all the servers.



---

**Note** If your Cisco Unified Communications Manager does not have the required device pack to support this firmware release, the firmware may not work correctly.

---

For information on the Cisco Unified Communications Manager Device Packs, see [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/compat/matrix/CMDP\\_BK\\_CCBDA741\\_00\\_cucm-device-package-compatibility-matrix.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/matrix/CMDP_BK_CCBDA741_00_cucm-device-package-compatibility-matrix.html).

## Install Firmware Release 11.0(5)SR1 on Cisco Communications Manager Express

You must download the Cisco Wireless IP Phone 8821 firmware image file from the software download center.

For information on Cisco Unified Communications Manager Express support, see [http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucme/feature/phone\\_feature/phone\\_feature\\_support\\_guide.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/feature/phone_feature/phone_feature_support_guide.html).

For more information about this procedure, refer to the “Install and Upgrade Cisco Unified CME Software” chapter in the *Cisco Unified Communications Manager Express System Administrator Guide* at this URL:

[http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucme/admin/configuration/manual/cmeadm.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/admin/configuration/manual/cmeadm.html)

### Procedure

---

- Step 1** Go to the following URL:  
<https://software.cisco.com/download/home/284729655>
- Step 2** Choose **Wireless IP Phone 8821** or **Wireless IP Phone 8821-EX**.
- Step 3** Choose **Session Initiation Protocol (SIP) Software**.
- Step 4** Choose **11.0(5)SR1** in the **Latest Releases** folder.
- Step 5** Click **Download** or **Add to cart** and follow the prompts.  
The file to download is `cmterm-8821.11-0-5SR1-4.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.
- 

## Install Firmware Release 11.0(5)SR1 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.

### Procedure

---

- Step 1** Go to the following URL:  
<https://software.cisco.com/download/home/284729655>
- Step 2** Choose **Wireless IP Phone 8821** or **Wireless IP Phone 8821-EX**.
- Step 3** Choose **Session Initiation Protocol (SIP) Software**.
- Step 4** In the **Latest Releases** folder, choose **11.0(5)SR1**.
- Step 5** Select the firmware file, click the **Download** or **Add to cart** button, and follow the prompts.  
Firmware file: `cmterm-8821-sip.11-0-5SR1-4.k3.cop.sgn`

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

- Step 6** Click the + next to the firmware file name in the Download Cart section to access additional information about this file. The hyperlink for the readme file is in the Additional Information section, which contains installation instructions for the corresponding firmware.
- Step 7** Follow the instructions in the readme file to install the firmware.
- 

## Limitations and Restrictions

### Phone Behavior During Times of Network Congestion

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 (Unified CM). Change the field from the default of 100 to 20.

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

For more information, look at CSCvc14605 using <https://tools.cisco.com/bugsearch>.

### 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 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=286308995&rls=11.0%285%29SR1&sb=anfr&bt=custV>
  - Use this URL for all open caveats:  
<https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=286308995&rls=11.0%285%29SR1&sb=af&bt=custV>
  - Use this URL for all resolved caveats:  
<https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=286308995&rls=11.0%285%29SR1&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 Wireless IP Phone 8821 that use Firmware Release 11.0(5)SR1.

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](#).

- CSCuw10789 Configuration: RTP/sRTP Port Range Configuration
- CSCvh27418 Transfer soft key shall be grey before C answer while semi-transfer is disabled
- CSCvh47665 No Secure tone played on protected phones while enable speaker
- CSCvi80433 Phone doesn't process the EAP request frame, causing de-registration
- CSCvj31950 Intermittent "\"Device or resource busy\" can still happen
- CSCvk22665 8821 display comes on sometimes when on call with shared line
- CSCvk59324 CCKM roaming failure then call dropped on roaming stress test bed
- CSCvm04637 Continuous scan busy is reproducible on Conducted test bed
- CSCvm58907 Firmware sometimes couldn't complete the fresh association
- 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.

- CSCvm87368 Phone can't get ip address when DHCP option 150 field configured with MaxLength
- CSCvm91475 Can't answer incoming call for a while when hold reversion is 20s with about 20 call sessions
- CSCvm94269 DTIM period in WLAN Diags shows as 3 sometimes
- CSCvm95611 XML message does not display on lock screen if http url priority is 1 or 2
- CSCvn05182 UI error while enable FAC
- CSCvn07039 "Error:Invalid Code in Speed dial" not display while press SD including error FAC or CMC
- CSCvn18501 MLPP priority lost in session bubble during xfer/conference
- CSCvn41362 cp8821i¼šno "CAL Text#" displayed in "incoming call toast"
- CSCvn42965 Ring Setting of Busy Station set to Ring not work on 8821
- CSCvn43154 No "details" softkey in multi-leg call history
- 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
- CSCvn64510 Neighbor list shows multiple AP's and does not update when in Single AP mode
- CSCvn66303 Phone not vibrate while with hold or RIU session when vibrate on ring:on
- CSCvn81608 Java process sometimes has significant delay in receiving events from wlanmgr after OOR & In Range
- CSCvo02996 "Call transferred" prompted when just making a call out
- CSCvo03077 Conference call still in held mode when all the other parties ended the call
- CSCvo05996 No Recording Tone heard after hold/resume several times.
- CSCvo09354 No toast message displayed after unchecking "Logged into Huntgroup" checkbox
- CSCvo26159 8821 failing to roam flexconnect over the air after reassoc\_resp it tries to auth with previous AP
- CSCvo30508 Softkey options shouldn't be shown in line missed calls page if blank
- CSCvo32881 Both speaker icon displayed when setting auto answer with speaker on shared line
- CSCvo37017 The ring doesn't play when a call in hold revert
- CSCvo44285 Multiple Vulnerabilities in qt
- CSCvo45811 Multiple Vulnerabilities in glibc
- CSCvo46442 Phone shut down when battery was showing 13%
- CSCvo55873 CFW info on non-primary line shall not be carried to SRST
- CSCvo74044 Hear short sharp ring tone during hold revert with Chirp1&2 ringtone and RIU session.

- CSCvo74177 Sometimes(90%) ringer is very small in hold reversion state when ringer volume is maximized
- CSCvo78333 Conference call UI display error on SRST
- CSCvo82607 Wrong behavior after press red key on originator phone in conference call when failover to SRST
- CSCvp02109 UI got into abnormal state after exiting PRT prior to completion then back to Settings when done
- CSCvp07713 WLAN diag not showing 2.4GHz AP's in WLAN profile set for 2.4GHz
- CSCvp14422 Phone will not roam from 5GHz WLAN profile to 2.4GHz WLAN profile if SSID disabled via WLC
- CSCvp31145 Stuttering audio quality with power save enabled
- CSCvp46085 Power button not working when initiating upgrade on multiple phones
- CSCvp63439 Vulnerabilities in wlan firmware: EAPOL M3 Embedded GTK : double buffer overflow
- CSCvq19702 Evaluation of sl-wireless-phones for TCP\_SACK
- CSCvq31290 BusyBox add\_match Function Arbitrary Code Execution Vulnerability
- CSCvq37631 After going Out of Range and re-registering the phone shows the line label as ????
- CSCvq42948 8821 phones are not able to renew LSC certificates via SCEP
- CSCvq48506 8821 Intermittent network busy and ps-poll versus UAPSD power save mode

## Resolved Caveats

The following list contains the severity 1, 2, and 3 defects that are resolved for the Cisco Wireless IP Phone 8821 that use Firmware Release 11.0(5)SR1.

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 resolved at the time this report was compiled. For an updated view of resolved defects or to view specific bugs, access the Bug Search Toolkit as described in [View Caveats, on page 5](#).

- CSCvp24305 Battery voltage exceeds the maximum voltage in certain stress test situations

## Cisco Unified Communication Manager Public Keys

To improve software integrity protection, new public keys are used to sign cop files for Cisco Unified Communications Manager Release 10.0.1 and later. These cop files have “k3” in their name. To install a k3 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 this additional cop file must first be installed 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 <https://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245>, 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 <https://cisco.com/go/phonefirmwaresupport>.

---

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](http://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)

© 2019–2020 Cisco Systems, Inc. All rights reserved.