Cisco Wireless IP Phone 8821 and 8821-EX Release Notes for Firmware Release 11.0(5)SR2

First Published: 2020-01-30

Last Modified: 2020-08-12

Cisco Wireless IP Phone 8821 and 8821-EX Release Notes for Firmware Release 11.0(5)SR2

These release notes support the Cisco Wireless IP Phone 8821 and 8821-EX Firmware Release 11.0(5)SR2.

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

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.

Install Firmware Release 11.0(5)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.

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)SR2**.

Step 5 Select the firmware file, click the **Download** or **Add to cart** button, and follow the prompts.

Firmware file: cmterm-8821.11-0-5SR2-2.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.

Install Firmware Release 11.0(5)SR2 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.

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

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)SR2** in the **Latest Releases** folder.

Step 5 Click **Download** or **Add to cart** and follow the prompts.

The file to download is cmterm-8821.11-0-5SR2-2.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, 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%29SR2&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%29SR2&sb=afr&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%29SR2&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)SR2.

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 4.

- 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
- CSCvm58907 Firmware sometimes couldn't complete the fresh association
- CSCvm87368 Phone can't get ip address when DHCP option 150 field configured with MaxLength
- CSCvm95611 XML message does not display on lock screen if http url priority is 1 or 2
- 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 cp8821Ã”Â°Ã¶no \"CAL Text#\" displayed in \"incoming call toast\"
- CSCvn43154 No \"details\" softkey in multi-leg call history
- 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
- 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

- CSCvo37017 The ring doesn't play when a call in hold revert
- CSCvo45809 OpenSSH Bailout Delaying User Enumeration Vulnerability (CVE-2018-15473)
- CSCvo55873 CFW info on non-primary line shall not be carried to SRST
- CSCvo78333 Conference call UI display error on SRST
- CSCvq25311 Multiple Vulnerabilities in dbus
- CSCvq31290 BusyBox add_match Function Arbitrary Code Execution Vulnerability
- CSCvq76705 Observe battery level 99%~100% floating issue after fully charged
- CSCvq80441 Cisco 8821 Wireless IP Phone Key Negotiation of Bluetooth Vulnerability
- CSCvr06067 Dnsmasq DNS Packet Processing Buffer Overflow Vulnerability
- CSCvr30314 Multiple Vulnerabilities in linux kernel (CVE-2019-10638 and CVE-2019-10639)
- CSCvr54353 Linux Kernel CVE (CVE-2019-16413 to CVE-2019-3874)
- CSCvr55596 cURL and libcurl tftp_receive_packet() Function Heap Buffer Overflow ...
- CSCvr57950 Phone continues blinking amber after shared line answers 2nd incoming call
- CSCvr70039 Vulnerability in linux kernel (CVE-2019-11190)
- CSCvr71242 Vulnerability in linux kernel (CVE-2019-11599)
- CSCvr71414 Vulnerability in linux kernel (CVE-2019-15214)
- CSCvr76650 Vulnerability in linux kernel (CVE-2019-15916)
- CSCvr87703 Vulnerability in linux kernel (CVE-2019-15666)
- CSCvr89188 Vulnerability in linux kernel (CVE-2019-16994)
- CSCvr94805 Vulnerability in linux kernel (CVE-2019-15927)
- CSCvs33435 Linux Kernel Use-After-Free Vulnerability CVE-2017-10661
- CSCvs55658 Multiple Vulnerabilities in openssl
- CSCvs63233 Multiple Vulnerabilities in linux_kernel CVE-2018-5344

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)SR2.

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 4.

- CSCvp31145 Stuttering audio quality with power save enabled
- CSCvp35700 wlanmgr debugs is not covered in telephony log profile

- CSCvp63439 Vulnerabilities in wlan firmware: EAPOL M3 Embedded GTK : double buffer overflow
- CSCvq19702 Evaluation of sl-wireless-phones for TCP_SACK
- CSCvq21067 8821 sending 405 NOTIFY for XML alert notifications requiring more than 5 seconds to complete
- 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
- CSCvq63813 8821 Wireless IP phone with shared line not showing conference/transfer softkeys when being on call
- CSCvq82571 Shared line displays incorrect call view when pressing Transfer or Conference softkey while on call
- CSCvq95752 Phone de-registered from CUCM due to the \"Unusual continuous EBUSY error\"
- CSCvr16492 One way audio on CP-8821 phones after RTP sequence number reset / rollover during active call
- CSCvr26925 Garbled audio when using max volume while docked
- CSCvr51045 8821 : PEAP authentication fails intermittently
- CSCvr73405 WLAN stops responding due to session timeouts
- CSCvr96070 Cisco Voice over IP Phone Remote Code Execution and Denial of Service Vulnerability
- CSCvr96103 Cisco Voice over IP Phone CDP Broadcast Issue
- CSCvs05461 8821 intermittently responds with NOTIFY 405 error code due to race condition between two timers

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.