Cisco IP Phone 8800 Series Multiplatform Phones Release Notes for Firmware Release 11.1(1)SR2

First Published: 2018-08-03

Release Notes

Use these release notes with the following Cisco IP Phone 8800 Series Multiplatform Phones running SIP firmware release 11.1(1)SR2.

- Cisco IP Phone 8811, 8841, 8851, and 8861 Multiplatform Phones
- Cisco IP Phone 8845 and 8865 Multiplatform Phones

The following table describes the individual phone requirements.

Phone	Support Server
Cisco IP Phone 8800 Series Multiplatform Phones	BroadSoft BroadWorks 22.0 MetaSphere CFS version 9.4 Asterisk 11.0

Related Documentation

Use the following sections to obtain related information.

Cisco IP Phone 8800 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/products/collaboration-endpoints/unified-ip-phone-8800-series/index.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

New and Changed Features

New Domain Support while Provisioning

When a phone connects to a network for the first time or after a factory reset, if there are no DHCP options setup, it contacts a device activation server for zero touch provisioning. Starting with this firmware release, phones will use activate.cisco.com instead of webapps.cisco.com for provisioning. Phones with older versions

of the firmware will continue to use webapps.cisco.com. Cisco recommends that you allow both the domain names through your firewall.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Provisioning Guide*

Upgrade the Firmware

Two firmware images are available for Cisco IP Phone 8800 Series Multiplatform Phones:

- Firmware for Cisco IP Phone 8811, 8841, 8851, and 8861 Multiplatform Phones (Audio only)
- Firmware for Cisco IP Phone 8845 and 8865 Multiplatform Phones (Video)

After the firmware upgrade completes, the phone reboots automatically.

Procedure

Step 1 Click the following URL:
https://software.cisco.com/download/home/286311392

Step 2 In the middle pane, select **IP Phone 8800 Series With Multiplatform Firmware**.

Step 3 Select your phone model in the right pane.

Step 4 On the next page that is displayed, select **Multiplatform Firmware**.

Step 5 On the next page that is displayed, in the **All Releases** > **MPP v11** folder, select **11.1.1 MSR2-1**.

Step 6 (Optional) Place your mouse pointer on the file name in the right pane, to see the file details and checksum values.

Step 7 Download the file:

- For Cisco IP Phone 8811, 8841, 8851, and 8861 Multiplatform Phones: `cp-88xx.11-1-1MSR2-1_REL.zip`
- For Cisco IP Phone 8845 and 8865 Multiplatform Phones: `cp-8845_65.11-1-1MSR2-1_REL.zip`

Step 8 Click **Accept License Agreement**.

Step 9 Unzip the files.

Step 10 Place the files in the TFTP, HTTP, or HTTPS download folder, depending on the protocol that you want to use for the upgrade.

Step 11 You can upgrade the phone firmware using either of the following methods.

- Upgrade the phone firmware from the phone administration web page:
  1. On the phone administration web page, go to **Admin Login** > **Advanced** > **Voice** > **Provisioning** tab, **Firmware Upgrade** section. In the **Upgrade Rule** field, enter the load file URL as described below.

     Load file URL format:

     ```
     <upgrade protocol>://<server ip address>[:<port>]>/<path>/<file name>.loads
     ```

Example:

```
https://10.73.10.223/firmware/sip88xx.11-1-1MSR2-1.loads
```

2. Click **Submit All Changes**.

- Upgrade the phone firmware directly from your web browser:

  In the address bar of your web browser, enter the phone upgrade URL as described below.

  Phone upgrade URL format:

  ```
  <phone protocol>://<phone ip address[:port]>/admin/upgrade?<load file URL>
  ```

  Load file URL format:

  ```
  <upgrade protocol>://<server ip address>[:<port>]>/<path>/<file name>.loads
  ```

  Example:

  ```
  https://10.74.10.225/admin/upgrade?https://10.73.10.223/firmware/sip88xx.11-1-1MSR2-1.loads
  ```

Note Specify the `<file name>.loads` file in the URL. The `<file name>.zip` file contains other files.

Limitations and Restrictions

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone voice 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:

- Administrative tasks, such as an internal port scan or security scan
- Attacks that occur on your network, such as a Denial of Service attack

Caller Identification and Other Phone Functions

Caller identification or other phone functions have not been verified with third-party applications for the visually or hearing impaired.

No Beep Sound Heard when the Mute Key is Pressed

When you press the **Mute** button during a call, you may not hear a beep sound. For anyone who is visually impaired, press the **Mute** button once to mute the phone and press the button twice to unmute the phone.

Phone Has a Firmware Build Earlier than 11.0.0

Sometimes, a phone taken out of the box has a firmware build earlier than 11.0.0. When this happens, you must upgrade the firmware on your phone to 11.0.0. Then you must update to 11.1.1 or later before you provision it.

Caveats

View Caveats

You can search for caveats using the Cisco Bug Search tool.

Known caveats (bugs) are graded according to severity level, and are either open or resolved.

Before you begin

To view the 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:

- To find all caveats, use this URL:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311392&sb=anfr&bt=custV
- To find all open caveats, use this URL:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311392&sb=anfr&sts=open&bt=custV
- To find all resolved caveats, use this URL:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311392&sb=anfr&sts=fd&bt=custV

Step 2 When prompted, log in with your Cisco.com user ID and password.

Step 3 (Optional) For information about a specific caveat, enter the bug ID number (*CSCxxnnnnn*) in the **Search for** field, and press **Enter**.

Open Caveats

The following list contains the severity 1, 2, and 3 caveats that are open for the Cisco IP Phone 8800 Series Multiplatform Phones that use the firmware release 11.1(1)SR2.

This list reflects a snapshot of the caveats that were open at the time this report was compiled. The status of caveats may have changed since then. For an updated view of the open caveats, or to view details or history for specific caveats, access the Bug Search Toolkit as described in View Caveats, on page 4. You must be a registered Cisco.com user to access this information.

- CSCvg00958 Phone doesn't send 420 Bad Extension when receives INVITE with unsupported value.
- CSCvg10304 Dual Mode and IP Pref is IPv4, Phone does not fall back to IPv4 address when IPv4 is up.

- CSCvg59538 No record in reboot reason when the reboot is triggered by a VLAN change in IPv6-only mode.
- CSCvg61134 Report delta has a speed dial parameter in the first time after factory reset.
- CSCvg61600 Geolocation status messages show up in English words with other locale.
- CSCvg63918 Phone still uses the old device after changing preferred audio device in ringback status.
- CSCvg70042 Wrong LED when DUT is configured call park shared-line ext function with wrong IP as PROXY.
- CSCvg73078 Call cannot be established on dialing out a speed dial when URI dialing and outbound proxy are set.
- CSCvg75579 Resync failed while using Digest Authentication with valid long password and username.
- CSCvg75733 The caller's ID shows "Anonymous" in a short time before picking up the call.
- CSCvg77675 Select line key fails when barge fails.
- CSCvg79273 The on-going call turn to single-pass after phone roamed to another AP by powering off current AP.
- CSCvg83031 Call center queue states cannot show "full", when queue threshold is exceeded.
- CSCvg84786 Provisioning Status shows incorrect while use no <flat-profile> in resync file.
- CSCvg96811 Hoteling subscribe will not retry after server unreachable or response error.
- CSCvg99367 Phone may reboot when changing to a non-exist language from web page.
- CSCvh06863 PLK (blf+cp) will pick up the caller in ringback state.
- CSCvh13270 Display is showing two calls during conference.
- CSCvh13556 Parameter RTP Packet Size validation does not work.
- CSCvh13736 Phone can't choose the language when just modifying the "d1".
- CSCvh15538 Video path is not available on DUTA when DUTB exits the early conference before DUTC answers. [8845 and 8865 only]
- CSCvh16152 MOS data is all zeroes in first second, phone should not send out this invalid data.
- CSCvh16923 When making an AMR-WB call, coding mode cannot be changed for AMR-WB codec. [8845 and 8865 only]
- CSCvh17018 The second busy line can't forward when active call forward busy by pressing *90 (star code).
- CSCvh17328 Recent call xmpp status is not updated when change xmpp presence to offline.
- CSCvh17346 Configuration, "Login Invisible" does not work when user login.
- CSCvh19110 Save "display brightness" in LCD GUI will be wrong value after submitting it in web GUI.
- CSCvh19488 Generate PRT will make phone reboot when "PRT Upload Rule" can't queried by DNS in HK locale.
- CSCvh23468 RFC2833 DTMF digits failing with AMR-WB mode.

- CSCvh29624 Phone does not preserve the existing call when on secondary SBC and failover to primary SBC.
- CSCvh52720 Ignore group paging on active call cannot work.
- CSCvh52884 Paging call can be answered when paging service disabled.
- CSCvh65657 The headset items are not aligned with the other items on the headset info UI.
- CSCvh66529 Phone reboots - Not handling multipart-mixed and multipart-related MIME type properly.
- CSCvh71029 Change of Hold Reminder Timer by resync causes phone to reboot.
- CSCvh71043 Phone reboots after received illegal value % for parameter.
- CSCvh67243 Speaker LED will not light when picking up a call.
- CSCvh72506 Phone doesn't use the last DNS cached record if TTL expires and no response from DNS server.
- CSCvh73357 Video does not always present. [8845 and 8865 only]
- CSCvh76496 Phone cannot get the correct content from HTTP 301 response.
- CSCvh76520 Phone always reports download fail when receive 301 after reboot.
- CSCvh76689 Phone cannot handle the content from HTTP 302 response.
- CSCvh76791 Provisioning status is wrong when receiving 500/501/503 response.
- CSCvh77161 Call center Disposition code sent to BS server mismatch the DispostionCode set.
- CSCvh78587 Phone can't accept a long realm in 401 when upgrade.
- CSCvh78730 Callee side has no video after pressing hold/resume with Asterisk call server. [8845 and 8865 only]
- CSCvh78875 The first frame of video is black screen after hold/resume one call with Asterisk call server. [8845 and 8865 only]
- CSCvh80117 Upgrade rule with macro conditional expression $SWVER does not equal distinguish phone model.
- CSCvh80256 Call UI only has hold and End call softkey after video disabled. [8845 and 8865 only]
- CSCvh86427 Phone reboots occasionally when switching the phone between power-adapter and POE. [8845 and 8865 only]
- CSCvh87790 Dual-mode phone should try IPv4 to upload PRT if no IPv6 address defined.

Resolved Caveats

The following list contains the severity 1, 2, and 3 caveats that are resolved for the Cisco IP Phone 8800 Series Multiplatform Phones that use Firmware Release 11.1(1)SR2.

This list reflects a snapshot of the caveats that were resolved at the time this report was compiled. The status of caveats may have changed since then. For an updated view of the resolved caveats, or to view details or history for specific caveats, access the Bug Search Toolkit as described in View Caveats, on page 4. You must be a registered Cisco.com user to access this information.

- CSCvh16689 PRT failing to upload into server since reply code 204 handled as failure
- CSCvh98841 7861 Key System scenarios STILL suffers serious issue (keys in stuck state, phone resets)
- CSCvh73377 7861 Key System scenarios suffers serious delays with Broadworks call control
- CSCvi47436 CP-8861-3PCC - Daylight Savings Time did not take effect after DST started
- CSCvi60903 Search in NAB: wrong character(rectangle) displayed at the end of directory result
- CSCvi20334 No Call Wait tone in secured call
- CSCvi18914 88xx-3PCC: 8851 losing audio with BroadCloud
- CSCvj84294 Can not open phone's web page with Chrome

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.

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: www.cisco.com go trademarks. 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)

© 2018 Cisco Systems, Inc. All rights reserved.