Cisco IP Phone 6800 Series Multiplatform Phones Release Notes for Firmware Release 11.1(2)SR1

First Published: 2018-08-31

Cisco IP Phone 6800 Series Multiplatform Phones Release Notes for Firmware Release 11.1(2)SR1

Use these release notes with the following Cisco IP Phone 6800 Series Multiplatform Phones running SIP Firmware Release 11.1(2)SR1.

- Cisco IP Phone 6841 and 6851 Multiplatform Phones

The following table describes the individual phone requirements.

Phone	Support Requirements
Cisco IP Phone 6800 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 6800 Series Documentation

See the publications that are specific to your language, phone model, and multiplatform firmware release. Navigate from the following Uniform Resource Locator (URL):

https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-phone-6800-series-multiplatform-firmware/tsd-products-support-series-home.html

New and Changed Features

The following sections describe the features that are new or have changed in this release.

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 6800 Series Multiplatform Phones Provisioning Guide*

Upgrade the Firmware

The Cisco IP Phone 6800 Series Multiplatform Phones support a single image upgrade using the TFTP, HTTP, or HTTPS protocols with a URL.

After the firmware upgrade completes, the phone reboots automatically.

Procedure

Step 1 Click the following URL:

https://software.cisco.com/download/navigator.html?mdfid=286318380&i=rm

Step 2 Choose **IP Phone 6800 Series with Multiplatform Firmware** in the middle pane.

Step 3 Choose your phone model in the right pane.

Step 4 Choose the **Multiplatform Firmware** software type.

Step 5 Under **Latest**, choose the **11.1.2 MSR1-1** folder.

Step 6 (Optional) Place your mouse pointer on the filename to display the file details and checksum values.

Step 7 Download the `cp-68xx.11-1-2MSR1-1_REL.zip` file.

Step 8 Click **Accept License Agreement** when you accept the Cisco End User License.

Step 9 Unzip the firmware files.

Step 10 Put the files in the TFTP, HTTP, or HTTPS download directory.

Step 11 Configure the **Upgrade Rule** on the **Provisioning** tab in the web page with the valid URL.

Use the URL format—`<protocol>://<serv_ip[:port]>/<filepath>/sipxxx.loads`

You can also upgrade the third-party call control by using a URL in the web browser—

`<protocol>://<serv_ip[:port]>/<filepath>/sipxxx.loads`

Example

`https://10.74.10.225/firmware/sip68xx.11-1-2MSR1-1.loads`

Note Use the `*.loads` file in the URL. The `*.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.

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 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=286318380&rls=11.1(2)&sb=anfr&bt=custV

- To find all open caveats, use this URL:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286318380&rls=11.1(2)&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=286318380&rls=11.1(2)&sb=anfr&sts=fd&bt=custV

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

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

Open Caveats

The following list contains the severity 1, 2, and 3 defects that are open for the Cisco IP Phone 6800 Series Multiplatform Phones that use Firmware Release 11.1(2)SR1.

For more information about an individual defect, you can access the online history for the defect by accessing the Bug Search tool and entering the Identifier. You must be a registered Cisco.com user to access this defect information.

Because the 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 the open defects or to view specific bugs, access the Bug Search Toolkit as described in the View Caveats, on page 3.

- CSCvi48553 Phone does not use right protocol to resync the configuration file when the DHCP option 159 is HTTP://ip1;ip2
- CSCvi50100 Phone software does not remove extra forward slash when the DHCP option 159 path ends with two forward slash characters.
- CSCvi60306 Phone cannot detect the new model key expansion module after an upgrade stress test is performed.
- CSCvi60396 DHCPv6 server provides 2 DNS servers; the phone screen LCD displays one DNS server, however the phone web page displays 2 DNS servers.
- CSCvi76172 Phone plays the wrong ringtone when you remove the URL from Ring7.
- CSCvi81274 Phone web GUI system information still displays the IPv4 NTP server when being changed to IPv6 only from dual-mode.
- CSCvi81457 Phone web GUI and phone screen GUI display wrong IPv4 gateway when DHCPv4 server is disabled while functioning.
- CSCvi81805 Phone web GUI and phone screen GUI display wrong IPv6 prefix length.
- CSCvi90086 BLF doesn't work when BLF List URI is xxxxx@ipv6_addr under IPv6 only mode.
- CSCvj37508 Phone rarely cannot detect KEM during long duration upgrade and downgrade test after 1000's of firmware upgrades.

Resolved Caveats

The following list contains the severity 1, 2, and 3 defects that are resolved for the Cisco IP Phone 6800 Series Multiplatform Phones that use Firmware Release 11.1(2)SR1.

For more information about an individual defect, you can access the online history for the defect by accessing the Bug Search tool and entering the Identifier. You must be a registered Cisco.com user to access this defect information.

Because the 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 the resolved defects or to view specific bugs, access the Bug Search Toolkit as described in the View Caveats, on page 3.

- CSCvj07154 CP-88xx-3PCC - Unable to hear beep from voicemail server
- CSCvj59089 Phone fails to provision using TR-69
- CSCvj84294 Can not open phone's web page with Chrome browser(Ver:67.0.3396.79)

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.