Cisco IP Phone 6800 Series Multiplatform Phones Release Notes for Firmware Release 11.3(7)

First Published: 2022-06-28

Release Notes

Use these release notes with the following Cisco IP Phone 6800 Series Multiplatform Phones running SIP Firmware Release 11.3(7).

- Cisco IP Phone 6821 Multiplatform Phones
- Cisco IP Phone 6841 Multiplatform Phones
- Cisco IP Phone 6851 Multiplatform Phones
- Cisco IP Phone 6861 Multiplatform Phones
- Cisco IP Phone 6871 Multiplatform Phones

Note This document doesn't include the DECT phones.

The following table describes the individual phone requirements.

Phone	Support Servers
Cisco IP Phone 6800 Series Multiplatform Phones	Cisco BroadWorks 24.0 MetaSphere CFS version 9.5 Asterisk 16.0

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

Direct PLK Configuration

You can directly perform the Programmable Line Key (PLK) configuration on a line key when the extension of the line key is still enabled. Before the firmware release 11.3(7), you must disable the line key extension for the PLK configuration.

To enable this feature, configure the parameter **Enable Direct PLK Configuration** under the **Miscellaneous Line Key Settings** section from **Voice** > **Phone** on the phone web interface. Also, ensure that the **Proxy** and **User ID** from **Voice** > **Ext** are empty.

Where to Find More Information

- *Cisco IP Phone 6800 Series Multiplatform Phones Administration Guide*
- *XML Reference Guide for Cisco IP Phone Multiplatform Phones*

HTTP Proxy Support

You can set up the phone to connect the Internet through a specified HTTP proxy server for security purposes. Your users can also set up a proxy server on the phone LCD UI. You can set up the proxy server by one of the proxy modes: Auto and Manual.

To enable this feature, you configure the parameters under the **HTTP Proxy Settings** section from **Voice** > **System** on the phone web interface.

Note Cisco IP Phone 6821 Multiplatform Phones partially supports the feature. For example, it doesn't support to upgrade by an HTTP proxy.

Where to Find More Information

- *Cisco IP Phone 6800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 6800 Series Multiplatform Phones User Guide*
- *XML Reference Guide for Cisco IP Phone Multiplatform Phones*

Inert Mode for PLK Configuration

You can set the Inert mode for a line key to completely shut it down. When set with the Inert mode, the line key doesn't provide any function for the users. You and your users can't use the line key for any purpose.

To use this feature, configure the parameter **Extended Function** of the disabled line key under the **Line Key (n)** section from **Voice** > **Phone** on the phone administration web page.

You can also apply this feature to the line keys on a key expansion module.

Where to Find More Information

- *Cisco IP Phone 6800 Series Multiplatform Phones Administration Guide*
- *XML Reference Guide for Cisco IP Phone Multiplatform Phones*

LDAP Search Enhancement

You can enable the unified search in the LDAP directory. The search allows you to enter any value as filters. You can search with first name, last name, extension, or phone number. The phone transfers the request as a single search request.

To enable this feature from the phone administration web page, use the **Unified Search Enable** parameter under the **LDAP** section from **Voice** > **Phone**.

Where to Find More Information

- *Cisco IP Phone 6800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 6800 Series Multiplatform Phones User Guide*

Login Credential for the Call Statistics Menu

Your phone has enhanced security for access to the **Call statistics** menu. If the user password is set, the users will be prompted to enter the password when they try to access the menu, in order to view the details of the recent calls.

Where to Find More Information

- *Cisco IP Phone 6800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 6800 Series Multiplatform Phones User Guide*

Spam Indication of Incoming Calls on the Phones

This release supports the new technology standard Secure Telephony Identity Revisited (STIR) and Signature-based Handling of Asserted information using toKENs (SHAKEN) for the Webex call logs, local call logs, and local call sessions when the phone is in Webex enviroment. STIR/SHAKEN has been mandated by Federal Communications Commission (FCC). These standards define procedures to authenticate and verify caller identification for calls carried over the IP network. The STIR-SHAKEN framework is developed to provide the end user with a great degree of identification and control over the type of calls they receive. These sets of standards are intended to provide a basis for verifying calls, classifying calls, and facilitating the ability to trust caller identity end to end. Illegitimate callers can easily be identified.

When STIR/SHAKEN support is implemented on the Webex server, the phone displays an extra icon next to the caller ID based on the caller's STIR/SHAKEN verification result.

Based on the verification result, the phone displays three types of icons.

Where to Find More Information

- *Cisco IP Phone 6800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 6800 Series Multiplatform Phones User Guide*

- *XML Reference Guide for Cisco IP Phone Multiplatform Phones*

VPN Connection Support

You can set up a VPN connection for the phone to connect to the network through a VPN server. Your users can also set up a VPN connection on the phone screen or the phone web page.

To enable this feature, you configure the parameters under the **VPN Settings** section from **Voice** > **System** on the phone web interface, and then reboot the phone to make the configurations take effect.

Note Cisco IP Phone 6821 Multiplatform Phones doesn't support the feature.

Where to Find More Information

- *Cisco IP Phone 6800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 6800 Series Multiplatform Phones User Guide*
- *XML Reference Guide for Cisco IP Phone Multiplatform Phones*

Multiplatform Phones Support Webex Call Logs

You can now enable a phone to support Webex call logs. The phone must onboards to Webex cloud to support this feature. When you enable this feature, the **Display recents from** menu under the **Recents** screen includes the **Webex** option in the calls list. The user then can set the option **Webex** to see the list of recent Webex calls.

To enable this feature from the phone administration web page, use the **Display Recents From** parameter under the **Call Log** section from **Voice** > **Phone**. Under the **Call Log** section, you must also enable the **CallLog Enable** parameter and select a phone line from **CallLog Associated Line** for which you want to display the Webex recent call logs.

Where to Find More Information

- *Cisco IP Phone 6800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 6800 Series Multiplatform Phones User Guide*
- *XML Reference Guide for Cisco IP Phone Multiplatform Phones*
- *Webex for Cisco BroadWorks Solution Guide*

Multiplatform Phones Support Webex Contacts

You can enable phone to support Webex contacts. The phone must onboards to Webex cloud to support this feature. You can also modify the Webex directory name. When you add support for Webex contacts, on the phone the user can see the Webex directory name under the **Directory** screen that you have created.

To enable this feature from the phone administration web page, use the **Directory Enable** parameter under the **Webex** section from **Voice** > **Phone**. To modify the Webex directory name, use the **Directory Name** parameter of **Webex** section.

Where to Find More Information

- *Cisco IP Phone 6800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 6800 Series Multiplatform Phones User Guide*
- *XML Reference Guide for Cisco IP Phone Multiplatform Phones*
- *Webex for Cisco BroadWorks Solution Guide*

Upgrade the Firmware

You can upgrade the phone firmware with TFTP, HTTP, or HTTPS. After the upgrade completes, the phone reboots automatically.

Procedure

Step 1 Click this link:

https://software.cisco.com/download/home/286318380

On the **Software Download** web page that is displayed, ensure that **IP Phone 6800 Series with Multiplatform Firmware** is selected in the middle pane.

Step 2 Select your phone model in the right pane.

Step 3 On the next page that is displayed, select **Multiplatform Firmware**.

Step 4 On the next page that is displayed, select **11.3.7** in the **All Releases** > **MPPv11** folder.

Step 5 (Optional) Place your mouse pointer on the file name to see the file details and checksum values.

Step 6 Download the corresponding file.

- 6821: `cmterm-6821.11-3-7MPP0001.272_REL.zip`
- Other phones in 6800 series: `cmterm-68xx.11-3-7MPP0001.272_REL.zip`

Step 7 Click **Accept License Agreement**.

Step 8 Unzip the file and place the files in the appropriate location on your upgrade server.

The appropriate location is the TFTP, HTTP, or HTTPS download folder, depending on the protocol that you want to use for the upgrade.

Step 9 Upgrade the phone firmware with one of these methods.

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

  Load file URL format:

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

Examples:

- 6821:

  `https://10.73.10.223/firmware/sip6821.11-3-7MPP0001.272.loads`

- Other phones in 6800 series:

  `https://10.73.10.223/firmware/sip68xx.11-3-7MPP0001.272.loads`

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

  Examples:

  - 6821:

    `https://10.74.10.225/admin/upgrade?https://10.73.10.223/firmware/sip6821.11-3-7MPP0001.272.loads`

  - Other phones in 6800 series:

    `https://10.74.10.225/admin/upgrade?https://10.73.10.223/firmware/sip68xx.11-3-7MPP0001.272.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 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.

Caveats

View Caveats

You can search for caveats (bugs) with the Cisco Bug Search tool.

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

Before you begin

You have your Cisco.com user ID and password.

Procedure

Step 1 Click one of the following links:

- To view all caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286318380&rls=11.3(7)&sb=anfr&bt=custV
- To view open caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286318380&rls=11.3(7)&sb=anfr&sts=open&bt=custV
- To view resolved caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286318380&rls=11.3(7)&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 defects that are open for the Cisco IP Phone 6800 Series Multiplatform Phones that use Firmware Release 11.3(7).

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 (*CSCxxnnnnn*). 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 7.

- CSCvx05369 KEM works slowly after add directories shortcut key to it
- CSCvw72979 Phone will show the call center softkey after answer executive or call forward call
- CSCvz35920 SSRC changes for outgoing Re-INVITES
- CSCwa70238 MPP should block sending CANCEL when Park button is pressed twice quickly

- CSCwb46008 Many PRTs with logs missing for around 5 seconds

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 11.3(7).

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 (*CSCxxnnnnn*). 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 7.

- CSCwb84017 68xx date overlaps cloud awareness icon when user pwd is set
- CSCwb02569 6821 Upgrade during network issues causes factory reset
- CSCwa61106 CP-6821-3PCC Wrong behavior in the HEAD method on 6821 phone when requesting firmware files
- CSCwb54978 CiscoIPPhoneStatus and CiscoIPPhoneStatusFile object is not mirrored in RTL mode
- CSCwb31031 Voicemail pin locked after unsuccessful login attempt by Hoteling Guest
- CSCwb23631 In German, department and email for directory are both displayed incorrectly
- CSCwa70835 When g722 is negotiated, the callee hears himself and the caller gets no audio
- CSCwa70820 MPP phones - Incorrect date and time in Recents page

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)