



Cisco IP DECT 6800 Series Release Notes for Firmware Release V0460 MSR1

First Published: 2019-07-09

Cisco IP DECT 6800 Series Release Notes for Firmware Release V0460 MSR1

These release notes support the Cisco IP DECT 6800 Series running Firmware Release V460 MSR1.

The Cisco IP DECT 6800 Series is compatible with the following systems:

- BroadSoft BroadWorks 21.0 and later
- Asterisk 13.1 and later

The firmware release versions are:

- Base station version: V0460 B0004
- Handset version: V0460 B0003

Related Documentation

Use the following sections to obtain related information.

Cisco IP DECT 6800 Series Documentation

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

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-dect-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.

Base Station Web Page Enhancements

This release contains the following enhancements to the base station administration web pages.

- The Syslog export file is formatted for better readability.
- The **Dial Plan** screen is enhanced for better readability.

Where to Find More Information

Cisco IP DECT 6800 Series Administration Guide

BroadSoft All Directory

Your users can search through individual BroadSoft directories or select **All** to search all available XML directories.

You must have the directory configured as an XML directory (**Central Directory > XML Server**). You enable one or more directories to display (Enterprise, EnterpriseCommon, Group, GroupCommon, Personal). The Group directory should be a subset of the Enterprise directory.

Where to Find More Information

- *Cisco IP DECT 6800 Series Administration Guide*
- *Cisco IP DECT 6800 Series User Guide*

Cisco Discovery Protocol Support

You can enable Cisco Discovery Protocol (CDP) on the Cisco IP DECT 6800 Series. CDP is a device-discovery protocol that runs on all Cisco equipment. It enables devices to communicate with other Cisco devices.

You enable CDP on the base station in the **Network Settings** web page.

Where to Find More Information

Cisco IP DECT 6800 Series Administration Guide

Handset User Interface Enhancements

Your users will see these changes.

- If users share lines, ...
- They can add recent callers to their local contacts list. When they do this, the number from the caller can be associated with the **Work**, **Home**, or **Mobile** field.
- When users delete existing entries in their Speed Dial list, they need to confirm or deny the deletion.
- If the incoming call information matches a content in the Directory, the information from the contact in the Directory displays in the **Recents** list.

Where to Find More Information

Cisco IP DECT 6800 Series User Guide

Serviceability Enhancements

This release includes the following Serviceability Enhancements:

- Ability to easily collect packet traces (PCAP logs) for troubleshooting.
- New base station out-of-box setup enhancements
- New handset out-of-box setup enhancements

- Provisioning enhancements
- To support failover better, the following new fields are available on the **Servers** administration web page:
 - Registration Retry Interval
 - Registration Retry Interval Long
 - Registration Retry RSC
- The base station can now configure with DHCP Option 66.

Where to Find More Information

- *Cisco IP DECT 6800 Series Administration Guide*
- *Cisco IP DECT 6800 Series User Guide*

Upgrade the Firmware

You can upgrade the base station and handset firmware with TFTP, HTTP, or HTTPS. You upgrade the base station first. After the upgrade, the base station automatically reboots. Then you upgrade the handsets, which automatically reboot.

You access the Cisco Software Download page to get the firmware in zip files. The zip files contain these firmware files:

- For the base station, the zip filename starts with `IPDECT-DBS210`.
- For the handset, the zip filename start with `IPDECT-PH6825`.



Note

- If you upgrade the base station from Firmware Release V460B1 or earlier, the administration user ID and password reset to the default values.
- After you install this load and then need to downgrade the release to Firmware Release V460B1 or earlier, you must perform a factory reset on the base station. This reset will set the administration user ID and password to the default values.

For detailed information about the upgrade procedure, refer to the “Maintenance” chapter in the *Cisco IP DECT 6800 Series Administration Guide*.

Before you begin

You need the TFTP, HTTP, or HTTPS server information.

Procedure

- Step 1** From your browser, go to <https://software.cisco.com/download/home/286323307>.
- Step 2** If required, sign in with your user ID and password.

- Step 3** Click **IP DECT 210 Multi-Cell Base-Station**.
 - Step 4** Select **Release 4.6**.
 - Step 5** Download the zip file for the required version.
 - Step 6** Return to <https://software.cisco.com/download/home/286323307>.
 - Step 7** Click **IP DECT 6825 with Multiplatform Firmware**.
 - Step 8** Select **Release 4.6**.
 - Step 9** Download the zip file for the required version.
 - Step 10** On your PC, unzip the files.
 - Step 11** Access the TFTP server file system.
 - Step 12** If not available, create a `Cisco` directory.
 - Step 13** Open the `Cisco` directory.
 - Step 14** Copy the new base station firmware file to the `Cisco` folder.
 - Step 15** Copy the new handset firmware file to the `Cisco` folder
 - Step 16** Complete the upgrade as described in the *Cisco IP DECT 6800 Series Administration Guide*.
-

Limitations and Restrictions

System Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone system voice 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.

Base Station Firmware Downgrade Limitation

After the upgrade for V460 B4, a downgrade of the base to a firmware version earlier than V460 B2 requires you to factory reset the base. This factory reset will reset the login credentials to the defaults. If you don't perform the factory reset, you can't log into the administration web pages.

Open Caveats

The following caveats are open at the time of the release.

- 243937 Holding tone not played
- 249149 Changes to extension not displaying, need to power cycle the handset.
- 251319 Handset turns on when placed in charger (previously turned off)

Resolved Caveats

The following caveats were resolved for the release.

- 209677 Save contact from recents doesn't work
- 213936 Delete existing entry in Speed Dial list doesn't ask for confirmation.
- 221378 CFNA is accepted with 0 Seconds
- 223476 Recents and Directory sync
- 223489 Syslog export format
- 223614 Error in upgrade screen message
- 223618 New Dial Plans screen – Scroll bars missing
- 224625 Base Station Admin Credentials - unable to change back
- 225085 [682x] AM/PM is not displayed on Time settings page
- 225116 682X:The alarm clock icon is not displayed
- 226735 No time out message “No BT devices found”
- 232747 Handset reset when scroll through XSI directory
- 233207 Interference noise on conference call on G722/G729
- 233352 BroadWorks XSI Directory crashing when scrolling through the contact list
- 233383 Query with 404 Not Found response
- 234116 Security Query regarding the WEB GUI
- 234544 Vibrate setting string change
- 235071 Not possible to search, when going from filtered search to no-filter search
- 238860 Provisioning Option 66
- 240004 Cannot select G726 codec on web page
- 244056 SRTP: No audio after Seq goes from 65535 to 0 and reINVITE
- 244266 Web page - Alarm Profile, Shared Call Appearance Settings
- 244269 Logs of download, etc are seen - But no configuration for it
- 244346 Direct access to get RSX and PCAP traces without login
- 246186 XSI Directory – Crash
- 248417 Statistics Export is not working
- 249828 OOB Issue - 0460 B2
- 250248 End of call - Pause Icon
- 258255 Unexpected reboot' seen in syslog after configuration loaded

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 NON-INFRINGEMENT 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: 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)

© 2019 Cisco Systems, Inc. All rights reserved.