Cisco IP DECT 6800 Series Release Notes for Firmware Release 5.1(2)

First Published: 2023-07-17

Last Modified: 2023-07-18

Cisco IP DECT 6800 Series Release Notes for Firmware Release 5.1(2)

These release notes support the Cisco IP DECT 6800 Series running Firmware Release 5.1(2).

This release supports the following devices:

- Cisco IP DECT 110 Single-Cell Base Station
- Cisco IP DECT 210 Multi-Cell Base Station
- Cisco IP DECT 110 Repeater
- Cisco IP DECT Phone 6823 Handset
- Cisco IP DECT Phone 6825 Handset
- Cisco IP DECT Phone 6825 Ruggedized Handset

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

- BroadSoft BroadWorks 22.0 and later
- Asterisk 13.1 and later

The firmware release versions are:

- Base station version 5.1(2): Displayed on the device as firmware version:
    - DBS-110: IPDect-DBS110_5-1-2MPP0001-4_REL.zip
    - DBS-210: IPDect-DBS210_5.1.2.MPP0001-4_REL.zip
- Handset version 5.1(2): Displayed on the device as firmware version:
    - 6823: IPDect-PH6823_5-1-2MPP0001-4_REL.zip
    - 6825: IPDect-PH6825_5-1-2MPP0001-4_REL.zip
    - 6825-RGD: IPDect-PH6825RGD_5-1-2MPP0001-4_REL.zip
- Repeater version 5.1(2): Displayed on the device as firmware version:
    - IPDect-RPT-110_5-1-2MPP0001-1_REL.zip

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

Cisco IP DECT Phone on CUCM

Now you can deploy Cisco IP DECT Phone 6825 on Cisco Unified Communication Manager. The Cisco IP DECT 6800 Series uses Digital Enhanced Cordless Telecommunications (DECT), a wireless technology. DECT operates at or near the 1.9 GHz frequency and does not interfere with other wireless technologies such as Bluetooth (operates at 2.5 GHz or 5 GHz). The Cisco IP DECT 6800 base station converts IP to DECT. The CUCM has no knowledge of the DECT operations. From the CUCM perspective, the DECT handsets appear as VoIP endpoints.

Note You must configure DECT base station for TCP. You must not use base station MAC address when you add the DECT to the CUCM. Each Cisco IP DECT Phone 6825 is a separate Third-party SIP device (advanced) on CUCM. For example, if you have 100 6825 handsets, then you will need 100 Third-Party SIP Device (Advanced) devices in CUCM.

Currently, few basic features such as make a call, answer a call, hold, transfer a call, conference are supported.

Where to Find More Information

- *Cisco IP DECT 6800 Series Administration Guide*
- *XML Reference Guide for Cisco IP DECT 6800 Series*

Configuration Changes Logging

Configuration changes logging feature lets you keep track of the configuration changes that the users make in the base station. You can also track configuration changes of a handset in the similar method. The base memory stores the information about which parameter is changed in the changelog. However, this information doesn't contain the actual details of the changes, but it only stores specific change made in the configuration. After the successful reporting of the changes, the changelog is cleared.

Where to Find More Information

- *Cisco IP DECT 6800 Series Administration Guide*
- *XML Reference Guide for Cisco IP DECT 6800 Series*

Configuration Change Reporting

When configuration changes of the base station is reported, the base station requests changelogs from the DECT locked handsets. For every locked handset, the base station requests three times with an interval of five seconds. Once requests for all handsets are complete, the changelogs of the base and the handsets are collected, processed, transformed to the correct XML tags. Then these tags are sent to the configuration server. If a handset doesn't respond, the syslog records this behavior. The handset changelogs from the device are cleared only after successful delivery of it to a base station.

Where to Find More Information

- *Cisco IP DECT 6800 Series Administration Guide*
- *XML Reference Guide for Cisco IP DECT 6800 Series*

EDOS Profile Supports all XML Parameters

Now the DECT base station is able to accept all XML parameters included in the configuration file from the Cisco CDA server (EDOS).

Where to Find More Information

- *Cisco IP DECT 6800 Series Administration Guide*

Stateful Firewall to Control Incoming Ethernet Traffic

Now for Cisco IP DECT 110 Single-Cell Base Station and Cisco IP DECT 210 Multi-Cell Base Station, you can enable stateful firewall to control incoming network traffic.

After the firewall is enabled, it analyzes ethernet packets of type IPv4. It then traces the trusted ports for incoming traffic and blocks data packtes from untrusted ports.

Where to Find more Information

- *Cisco IP DECT 6800 Series Administration Guide*
- *XML Reference Guide for Cisco IP DECT 6800 Series*

Network-Related Information Extraction Using CDP/LLDP

Both CDP and LLDP, which contain VLAN information, are included in this feature implementation. The protocols must be treated differently based on the different packet and content types.

Where to Find More Information

- *Cisco IP DECT 6800 Series Administration Guide*

Upgrade the Firmware

You can upgrade the base station and handset firmware with TFTP, HTTP, or HTTPS. You upgrade the base station first and then upgrade the handsets after the base station upgrade completes. The base station upgrade may take about 30 minutes to 1 hour to complete and reboot. The handset upgrade may take 20-30 minutes to download and verify, and an extra few minutes to load the new firmware file. The handset must be placed in the charger and not removed until the handset loads the firmware file and reboots.

You can upgrade Cisco IP DECT 210 Multi-Cell Base Station to Firmware Release 5.1(2) only if the base station is currently running release 5.0(1) or 4.8(1) SR1. If the base station is currently running release 4.7 or 4.8, you must upgrade the base station to release 5.0(1) or 4.8(1) SR1 before upgrading to release 5.1(2). If the base station is currently running release 4.5, you must upgrade the base station to release 4.6 in factory reset mode before upgrading to release 4.8(1) SR1.

You can upgrade Cisco IP DECT 110 Single-Cell Base Station to Firmware Release 5.1(2) if the base station is currently running release 5.0(1) or 4.8(1) SR1. If the base station is currently running release 4.8, you must upgrade the base station to release 5.0(1) or 4.8(1) SR1 before upgrading to release 5.1(2).

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-DBS110` for Cisco IP DECT 110 Single-Cell Base Station.
  - `IPDect-DBS210` for Cisco IP DECT 210 Multi-Cell Base Station.
- For the repeater, the zip filename starts with `IPDect-RPT-110`.
- For the handset, the zip filename starts with:
  - `IPDect-PH6823` for Cisco IP DECT Phone 6823 Handset.
  - `IPDect-PH6825` for Cisco IP DECT Phone 6825 Handset.
  - `IPDect-PH6825RGD` for Cisco IP DECT Phone 6825 Ruggedized Handset.

The Firmware Release 5.1 (2) zip files contain these files:

- Base station:
  - Cisco IP DECT 110 Single-Cell Base Station: `IPDect-DBS110_5-1-2MPP0001-4_REL.zip`
  - Cisco IP DECT 210 Multi-Cell Base Station: `IPDect-DBS210_5.1.2.MPP0001-4_REL.zip`
- Cisco IP DECT 110 Repeater: `IPDect-RPT-110_5-1-2MPP0001-1_REL.zip`
- Handsets:
  - Cisco IP DECT Phone 6823 Handset: `IPDect-PH6823_5-1-2MPP0001-4_REL.zip`
  - Cisco IP DECT Phone 6825 Handset: `IPDect-PH6825_5-1-2MPP0001-4_REL.zip`
  - Cisco IP DECT Phone 6825 Ruggedized Handset: `IPDect-PH6825RGD_5-1-2MPP0001-4_REL.zip`

Note

- If you haven't modified the password in the base station running Firmware version 4.8 or 4.8(1) SR1 and you upgrade the base station, the administration user ID and password change request displays when you login to the base station.
- From Firmware Release 5.1(2), if you need to downgrade to an earlier release, you can downgrade to the latest branch of the Firmware Release 5.0(1) or 4.8(1) SR1. You must perform a factory reset on the base station to downgrade. This reset will set the administration user ID and password to the default values.

For detailed information about the upgrade or downgrade 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 110 Repeater with Multiplatform Firmware**.

a) Select **All Release** > **MPP DECT v5** > **5.1.2**.
b) Download the zip file for the required version.
c) Return to https://software.cisco.com/download/home/286323307.

Step 4 Click **IP DECT 110 Single-Cell Base Station with Multiplatform Firmware**.

a) Select **All Release** > **MPP DECT v5** > **5.1.2**.
b) Download the zip file for the required version.
c) Return to https://software.cisco.com/download/home/286323307.

Step 5 Click **IP DECT 210 Multi-Cell Base Station with Multiplatform Firmware**.

a) Select **All Release** > **MPP DECT v5** > **5.1.2**.
b) Download the zip file for the required version.
c) Return to https://software.cisco.com/download/home/286323307.

Step 6 Click **IP DECT 6823 with Multiplatform Firmware**.

a) Select **All Release** > **MPP DECT v5** > **5.1.2**.
b) Download the zip file for the required version.
c) Return to https://software.cisco.com/download/home/286323307.

Step 7 Click **IP DECT 6825 with Multiplatform Firmware**.

a) Select **All Release** > **MPP DECT v5** > **5.1.2**.
b) Download the zip file for the required version.

   You can download both **IP DECT 6825 with Multiplatform Firmware** and **IP DECT 6825 Ruggedized with Multiplatform Firmware** from this page.

c) Return to https://software.cisco.com/download/home/286323307.

Step 8 Unzip the downloaded files to your computer.

Step 9 Access the TFTP server file system.

Step 10 If not available, create a `Cisco` directory.

Step 11 Open the `Cisco` directory.

Step 12 Copy the new base station firmware file to the `Cisco` folder.

Step 13 Copy the new handset firmware file to the `Cisco` folder.

Step 14 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.

After the upgrade to Firmware version 5.0(1), you can downgrade the base station only to the latest branch of the Firmware version 4.8(1) SR1. This downgrade requires you to factory reset the base station. The 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.

Base Station Alert Due to a Clock Synchronization Error

The base station self-check process fails if there’s a clock synchronization error. When this error occurs, the LED on the base station flashes red, amber, and green. In this case, we recommend the standard RMA process.

Open Caveats

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

- CSCwd83296 DECT 110/210: Handset Upgrade Rules can't be overwritten by blank rule from CM services.
- CSCwf36615 redundant SAC credentials sent by base
- CSCwf14341 DECT 6823 handset - 'Loud Ringer' melody not available for 'Contacts' configured in handset

- CSCwf42230 incorrect source SIP port used in contact header
- CSCwf83229 DECT base using ipv6 for resync when only ipv4 selected as <IP_mode>

Resolved Caveats

The following caveats were resolved for the release:

- CSCwd11394 Cannot login to DBS210 web GUI with correct Admin password
- CSCwd11388 All handsets deregister after performing any handset related operation from Control Hub
- CSCvz61849 Handset can not be associated with Alarm profile through config file
- CSCwd11390 No Geolocation header for emergency calls
- CSCwd25173 Feature pack is using lot of DECT resources
- CSCwd25148 Leak of Call Instances if no Response to Endpoint Request
- CSCwd25158 ROS2 mail queue full from Mac Interrupt observed in Autotest
- CSCwd25168 Update SCA icons are using a lot of DECT recources
- CSCwd25133 Full System test showed very slow FWU updates and UDP packet loss for base stations
- CSCwa93524 <Login_User_ID> needs to have a per line scope
- CSCwa15271 Calllog related parameters should be removed from the web UI and XML tokens
- CSCwa59141 CIAM: mbed-tls 2.23.0 upgrade to mbed-tls 2.28.0
- CSCwd25122 Restrict admin web UI login to a single active session by closing the previous session
- CSCwe69285 DBS110 dual cell should ignore chain ID sent in XML

Cisco IP Phone Firmware Support Policy

For information on the support policy for phones, see the Cisco IP Phone Firmware Support Policy.