Cisco IP Phone 8800 Series Multiplatform Phones Release Notes for Firmware Release 12.0(3)

First Published: 2023-07-21

Last Modified: 2023-07-21

Release Notes

Use these release notes with the Cisco IP Phone 8800 Series Multiplatform Phones running SIP Firmware Release 12.0(3).

The following table describes the individual phone requirements.

Phone	Support Requirements
Cisco IP Phone 8800 Series Multiplatform Phones	BroadSoft BroadWorks 24.0 MetaSphere CFS version 9.5 Asterisk 16.0

Related Documentation

Use the following sections to obtain related information.

Cisco IP Phone 8800 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/products/collaboration-endpoints/ip-phone-8800-series-multiplatform-firmware/index.html

New and Changed Features

Automatic Renewal of MIC Certificate

From 12.0.3 release onwards, all phones can automatically renew its Manufacture Installed Certificate (MIC) by reaching out to cloud service at sudirenewal.cisco.com. To allow traffic to the cloud service, make sure to update your firewall settings. If you are a service provider and your servers challenge phones for their certificate, make sure to update the server trust store to include new root CA. For more information, see the field notice FN - 72302 - https://www.cisco.com/c/en/us/support/docs/field-notices/723/fn72302.html.

Note From 12.0.3 release, SUDI feature is enabled by default.

Where to Find More Information

- *Cisco IP Desk Phone with Multiplatform Firmware (MPP) - Administration Guide*

Desk Booking for a Specific Duration

Now the user can reserve an available desk for a certain period of time depending on how many hours is required to get the work done. The user scans the QR code using the mobile phone and during the signing in process, a screen **Book this desk until** appears. In this screen, one can book a slot for the required working hours in the format of 12-hour or 24-hour. You configure this format from the phone web interface for your user.

You can use the **Time Format** parameter in the phone administration web page from **Phone** > **User** to configure the time format.

Where to Fine More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones User Guide*
- *Cisco IP Desk Phone with Multiplatform Firmware (MPP) - Administration Guide*
- *XML Reference Guide for Cisco IP Phone Multiplatform Phones*

Factory Reset with SIP-Notify

You can initiate a factory reset of a phone when the phone is deleted from server. Once deleted by the administrator, phone will receive SIP-NOTIFY message with event:factory-reset and performs factory-reset accordingly.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones User Guide*
- *Cisco IP Desk Phone with Multiplatform Firmware (MPP) - Administration Guide*

HTTPS Enablement by Default

With this release you must enable **`Https`** by default to access the phone administration web page. To enable this feature from the phone administration web page, use the **Enable Protocol** and **Web Server Port** under **System Configuration** section from **Voice** > **System**. A phone with Firmware version 12.0(3) and later always gets redirected to **`https://<ip address>:443`**. When you enable protocol to **`Https`** and web server port to **`443`**, after the factory reset, if you do not change the values and your user wants to access the phone administration web page with **`http://<ip address>`** or **`http://<ip address>:80`**, the URL gets redirected to **`https://<ip address>:443`**.

Where to Find More Information

- *Cisco IP Desk Phone with Multiplatform Firmware (MPP) - Administration Guide*

Invoking of XML Service with Multicast Paging

This feature allows phones to recieve pages from a server to optionally display an image or other UI elements. With this feature, you can invoke the XML service from multicast paging. When configured, user will not be able to see the **XML application** in the **Information and settings** menu on the phone.

To enable this feature from the phone administration web page, use the **XML Application Service URL** parameter under **XML Service** from **Voice** > **Phone**.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones User Guide*
- *Cisco IP Desk Phone with Multiplatform Firmware (MPP) - Administration Guide*

Key Expansion Module Key Supports SIP Line

Now, Cisco IP phone 8851, 8861, and 8865 support extension 1 to extension 16. You can enable any of these 16 extension numbers to a key expansion module line key so that the assigned line key can be used as a SIP line. Similarly phone line keys also support extension 1 to extension 16. Only audio key expansion module and video key expansion module support this feature.

To enable this feature from the phone administration web page, choose a key expansion module key and assign an extension number in the **Extension** parameter under **Voice** > **Att Console**.

Where to Find More Information

- *Cisco IP Desk Phone with Multiplatform Firmware (MPP) - Administration Guide*
- *XML Reference Guide for Cisco IP Phone Multiplatform Phones*

Out-Of-Box Device Onboarding with CDA Retry

To simplify the device onboarding experience and to make it more resilient against failures, retry provisioning with CDA (MAC address based zero touch provisioning service) is introduced. This retry provisioning is triggered during one of the following condition:

- When the phone is taken out-of-box for the first time and has firmware version 12.0.3 or later pre-installed.
- When the phone undergoes factory reset while running firmware version 12.0.3 or later.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones User Guide*
- *Cisco IP Desk Phone with Multiplatform Firmware (MPP) - Administration Guide*

Password Alert after Factory Reset

After a factory reset, when the phone boots up for the first time, it displays a prompt to set up a password as a security measure. If the user chooses to skip the password setup, phone shows a warning message. You can set the user password in the phone administration web page. If the password is not created, the user can use the **Create** softkey on the **Issues** screen to create a new password. Once the user creates the password the phone displays an unlock icon on the phone screen.

To enable this feature from the phone administration web page, use the **Display Password Warnings** parameter under **System Configuration** section from **Voice** > **System**.

Where to Find More Information

- *Cisco IP Desk Phone with Multiplatform Firmware (MPP) - Administration Guide*

Upgrade 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 8800 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 **12.0.3** in the **All Releases** > **MPPv12** 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.

- 8845 and 8865: `cmterm-8845_65.12-0-3MPP0001-87_REL.zip`
- Other phones in 8800 series: `cmterm-88xx.12-0-3MPP0001-87_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:

  - 8845 and 8865:

    ```
    http://10.73.10.223/firmware/sip8845_65.12-0-3MPP0001-87.loads
    ```

    ```
    https://server.domain.com/firmware/sip8845_65.12-0-3MPP0001-87.loads
    ```

- Other phones in 8800 series:

  `http://10.73.10.223/firmware/sip88xx.12-0-3MPP0001-87.loads`

  `https://server.domain.com/firmware/sip88xx.12-0-3MPP0001-87.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:

  - 8845 and 8865:

    `https://10.74.10.225/admin/upgrade?http://10.73.10.223/firmware/sip8845_65.12-0-3MPP0001-87.loads`

    `https://10.74.10.225/admin/upgrade?https://server.domain.com/firmware/sip8845_65.12-0-3MPP0001-87.loads`

  - Other phones in 8800 series:

    `https://10.74.10.225/admin/upgrade?http://10.73.10.223/firmware/sip88xx.12-0-3MPP0001-87.loads`

    `https://10.74.10.225/admin/upgrade?https://server.domain.com/firmware/sip88xx.12-0-3MPP0001-87.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 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.

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&rls=12.0(3)&sb=anfr&bt=custV&prdNam=Cisco%20IP%20Phone%208800%20Series%20with%20Multiplatform%20Firmware
- To view open caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&rls=12.0(3)&sb=afr&bt=custV&prdNam=Cisco%20IP%20Phone%208800%20Series%20with%20Multiplatform%20Firmware
- To view resolved caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&rls=12.0(3)&sb=fr&bt=custV&prdNam=Cisco%20IP%20Phone%208800%20Series%20with%20Multiplatform%20Firmware

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 8800 Series Multiplatform Phones that use Firmware Release 12.0(3).

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 6.

- CSCwe55809—Personal contact calls play the distinctive ring while there's an active call on 8800 phones.
- CSCwf15218—Vulnerabilities in curl - multiple versions CVE-2023-27534 and others.
- CSCwf15355—Vulnerabilities in curl - multiple versions CVE-2020-8177.
- CSCwf24915—8865 no video since srtpm_srtpifUnprotect failure after hold resume several times.

- CSCwf30157—Video phone: Camera led may be off in ad-hoc conference call.

Resolved Caveats

The following list contains the severity 1, 2, and 3 defects that are resolved for the Cisco IP Phone 8800 Series Multiplatform Phones that use Firmware Release 12.0(3).

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 6.

- CSCvb65980—Nav hard key can't move cursor in Search Enterprise Directory.
- CSCvy86354—MPP phones - 8845/8865 phones are randomly crashing
- CSCwa95349—Cloud awareness: Phone will create new registration after reboot or for each refresh request.
- CSCwb27243—8865 Crash - null pointer at libmmalvcp.so.
- CSCwb65913—ICE: Phone becomes not operational when Media ports are not getting released.
- CSCwb85883—88xx 88x5 the generated PRT toast content will overlap when a paging call is received.
- CSCwc08931—Cisco MPP 8851 IP Phone with Cisco 561 USB headset are randomly crashing.
- CSCwc29314—MPP phones (88xx/68xx/78xx) do not support dual registration with TCP.
- CSCwc61284—SSH is not available for phones running Multiplatform Phone (MPP) firmware.
- CSCwd01853—Cisco MPP Phones reboots when park and retrieve a call too fast.
- CSCwd47209—The 'ACK' from MPP phone does not have 'Route' header.
- CSCwd56139—Cisco MPP phones "Debug" level log still print out when log level set to "Notice".
- CSCwd62034—AWR-WB Media Type does not conform to RFC4867.
- CSCwd62809—Intermittent audio noises are heard on Webex calls.
- CSCwd86078—Vulnerabilities in u-boot - multiple versions CVE-2022-34835 cmd_i2c.c.
- CSCwd93487—8851 KEM Memory leak causing reboot.
- CSCwe01828—Vulnerabilities in linux-kernel - multiple versions CVE-2021-4037.
- CSCwe24803—Vulnerabilities in linux-kernel 4.9.118 CVE-2022-3643.
- CSCwe27819—Vulnerabilities in linux-kernel - multiple versions CVE-2016-0821.
- CSCwe38474—Held calls cannot resume on 8845/8865.
- CSCwe46272—MPP 12.x not properly optimizing media via ICE on calls to LGW.
- CSCwe46781— MPP 8865/8861 External Audio Output does not work after upgrade to 12.0.1.
- CSCwe67157—Vulnerabilities in linux-kernel - multiple versions CVE-2023-26545.

- CSCwe86166—'Transfer' softkey in the Connected Key List is not working in 11.3.5 or later releases.
- CSCwf17564—MPP - 8851 Phone lag/freeze on 12.0.1 Firmware.
- CSCwf23858—Self-view frozen for user in a 1:1 call.
- CSCwf35777—MPP - 88xx Inbound caller ID issue 12.0.1 Firmware.
- CSCwf82386—Expiring SUDI/MIC in MPP phones.
- CSCwh20086—MPP 8861+KEM restarts while idle.
- CSCwf35777—Inbound caller ID issue.
- CSCwh20086—MPP restarts randomly while idle.
- CSCwf29727—Hard transfer button does not transfer.
- CSCwf24303—8845/65 MPP Video blank during meeting - RTCP Packets dropped as malformed.
- CSCwh14446—MPP is losing registration randomly.

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.