Cisco IP Phone 8800 Series Multiplatform Phones Release Notes for Firmware Release 11.3(4)

First Published: 2021-06-15

Release Notes

Use these release notes with the Cisco IP Phone 8800 Series Multiplatform Phones running SIP Firmware Release 11.3(4).

The following table describes the individual phone requirements.

Phone	Support Requirements
Cisco IP Phone 8800 Series Multiplatform Phones	Cisco BroadWorks 24.0 MetaSphere CFS version 9.5 Asterisk 13.0

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

Headset Inventory Reporting

This feature enables the phone to report the peripheral information to the server. When configured, if you connect or disconnect a peripheral device, the phone reports a message to the server. The peripherals that are supported are KEM and Cisco headset.

To enable this feature, use the field **Peripheral Inventory Enable** under **Peripheral** section. You can access this section from **Voice** > **SIP** of the phone web interface.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*

RTL Language Support

With the firmware release 11.3(4), phone now supports Right-to-Left (RTL) languages. All multiplatform IP phones, A-KEM, and V-KEM now support the following languages.

- Arabic
- Hebrew

In the phone web interface, you can use the **Dictionary Server Script** field from **Voice** > **Regional** > **Language** to configure the language support.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*

SSRC Reset for the New RTP and SRTP Sessions

Enable the Synchronization Source (SSRC) reset and avoid a failed call transfer, where only one party on a transferred call hears the audio.

To enable the feature, use the **SSRC Reset on RE-INVITE** field under the **RTP Parameters** section from **Voice** > **SIP**.

Note By default, the SSRC reset is disabled for the new RTP and SRTP sessions.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*

Support Maximum of 12 SRV Records in a Query

The maximum number of the DNS SRV records supported in a query increases from 6 to 12.

Before the 11.3(4) release, the maximum number of the DNS SRV records is 6.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*

Unplanned Migration Prevention

When you install enterprise to MPP migration firmware COP files, the firmware files are available for use to specify as load name. You can then configure to retain the default **Load Information** value of the phone. As a result all the phones of the same model do not start migration process unintentionally. It allows you to change the default load manually.

Where to Find More Information

- *Cisco IP Phone 7800 and 8800 Series Migration Guide (On-Premises to Multiplatform Phones)*

- *Convert between Enterprise Firmware and Multiplatform Firmware for Cisco IP Phone 7800 and 8800 Series*

XMPP User ID Display

You can display the XMPP user ID with the highest priority on the phone screen.

When you enable the feature, the XMPP user ID overrides other names, for example, Station Name.

Note Before the release 11.3(4), the XMPP user ID overrides other display names by default. In this release, if you use the default setting, the XMPP user ID might not display on the phone screen as it's not set with the top priority. The top priority of displaying the XMPP user ID is disabled by default.

To enable this feature, you can use the **Display XMPP User ID With Top Priority** field under the **Broadsoft XMPP** section from **Voice** > **Phone**.

Where to Find More Information

- *Cisco IP Phone 8800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 8800 Series Multiplatform Phones User 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 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 **11.3.4** 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.

- 8845 and 8865: `cmterm-8845_65.11-3-4MPP0001-374_REL.zip`
- Other phones in 8800 series: `cmterm-88xx.11-3-4MPP0001-374_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_65.11-3-4MPP0001-374.loads
       ```

       ```
       https://server.domain.com/firmware/sip8845_65.11-3-4MPP0001-374.loads
       ```

     - Other phones in 8800 series:

       ```
       http://10.73.10.223/firmware/sip88xx.11-3-4MPP0001-374.loads
       ```

       ```
       https://server.domain.com/firmware/sip88xx.11-3-4MPP0001-374.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_65.11-3-4MPP0001-374.loads
    ```

    ```
    https://10.74.10.225/admin/upgrade?https://server.domain.com/firmware/sip8845_65.11-3-4MPP0001-374.loads
    ```

  - Other phones in 8800 series:

    ```
    https://10.74.10.225/admin/upgrade?http://10.73.10.223/firmware/sip88xx.11-3-4MPP0001-374.loads
    ```

    ```
    https://10.74.10.225/admin/upgrade?https://server.domain.com/firmware/sip88xx.11-3-4MPP0001-374.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:

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=286311392&rls=11.3(4)&sb=anfr&bt=custV
- To view open caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311392&rls=11.3(4)&sb=afr&bt=custV
- To view resolved caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311392&rls=11.3(4)&sb=fr&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 8800 Series Multiplatform Phones that use Firmware Release 11.3(4).

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 5.

- CSCvv51309 MPP software is not completing the ICE procedures when placing a call to L2SIP
- CSCvw72979 Phone will show the call center softkey after answer executive or call forward call.
- CSCvx44944 Short activation code taking a long time to get configurations
- CSCvx44952 Phone showing Failed to download configurations even when it was successful while migrating to MPP
- CSCvx49825 Phone stuck at configuration check in progress during firmware migration if it was on WiFi before
- CSCvx61001 Multiple Vulnerabilities in Frame Aggregation and Fragmentation Implementation of 802.11
- CSCvy20491 Customer enhancement requests for 3PCC feature: View image of IP camera on 3PCC phone.
- CSCvy36096 Unexpected 481 sent by phone when off/on-hook shared line quickly
- CSCvy39554 MPP Mutual auth fails in HTTPS for E911
- CSCvy27737 No reorder tone and will not time out when network conference fail
- CSCvy56034 ICE: Before complete transfer stay 12 min,one way video issue
- CSCvy58331 ICE: Call Pickup with a video phone fails intermittently for a video call after ICE complete

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 11.3(4).

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 5.

- CSCvv20301 POR: Not all characters are shown in the character preview pop-up
- CSCvv64780 Cannot restore the phone background after setting an invalid background picture
- CSCvv83242 Multiple Vulnerabilities in dnsmasq DNS Forwarder Affecting Cisco Products: January 2021
- CSCvw21396 ICE, Offer not having ICE candidates should be handled
- CSCvw42896 Phone can scan out the hidden SSID and appears in the scan list as a messy code
- CSCvw54519 Speed dial of 1 digit number is not supported for Proxy Call
- CSCvw69940 Evaluation of 8800 for Sweyntooth vulnerabilities in Bluetooth Low Energy
- CSCvw82717 MPP phones - SBC is rejecting a specific line-seize SIP SUBSCRIBE
- CSCvw87814 Dropped Media from ICE enabled Device on Non ICE Call Path
- CSCvx05499 Two "Anonymous" were shown on LCD when shareline reiceving anonymous calls
- CSCvx13295 xmpp ping error will not trigger failover
- CSCvx38703 Phone cold rebooting upon expiration of download timer
- CSCvx38710 Logs are lost upon cold reboot
- CSCvx47030 softkey is wrong on cfwd contacts selection page
- CSCvx62528 Cisco IP Phone Cisco Discovery Protocol Out-of-Bound Read Vulnerability
- CSCvx69154 MPP Not Setting "Don't Fragment" (DF) Bit
- CSCvx84314 Evaluation of 8800 for OpenSSL March 2021 vulnerabilities
- CSCvx85189 Shared line remaining red after user hangs up call.
- CSCvy30979 MPP phones not honouring PAID update for caller ID in certain cases

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.

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)