Cisco IP Conference Phone 8832 Multiplatform Phones Release Notes for Firmware Release 12.0(1)

First Published: 2023-01-18

Last Modified: 2023-01-17

Release Notes

Use these release notes with the Cisco IP Conference Phone 8832 Multiplatform Phones running SIP Firmware Release 12.0(1).

The following table describes the individual phone requirements.

Phone	Support Requirements
Cisco IP Conference Phone 8832 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 Conference Phone 8832 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 Feature

Display of Webex Call Duration

Now the phone displays the Webex call log duration. In the **Recents** screen, when you choose to view details of a placed call or a received call, the duration of the call is also displayed on the **Received calls** or **Placed calls** screen.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*

- *Cisco IP Conference Phone 8832 Multiplatform Phones User Guide*

FIPS Mode Enabling

You can now enable phone with Federal Information Processing Standards (FIPS) compliance. This validation is required after OpenSSL Cisco OpenSSL 7.2.440 is ported to SL 2.0 as secured communication system through cryptography is important.

To enable this feature from the phone administration web page, use **FIPS mode** parameter under the **Security Settings** section from **Voice** > **System**.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*
- *XML Reference Guide for Cisco IP Phone Multiplatform Phones*

Support for RFC-8760

The Cisco IP Phone now supports RFC-8760. If supported, the phone sends a SIP register request to the server without an authorization header field and the SIP server responses a 401 status with multiple www-authenticate headers. The headers include support for more secure digest algorithms such as SHA256, SHA-512/256 and MD5.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*

WxC Outbound Proxy Survivability Support

Phone now has the ability to register to the Site Survivability Gateway (SGW) nodes when WxC SSE nodes are unreachable. When the phone connects to SGW nodes, phone supports only limited set of calling features. When this feature is enabled, user can see a service interruption notification on the phone.

To enable this feature from the phone administration web page, use **Survivability Proxy**, **Survivability Proxy Fallback Intvl** parameters under the **Proxy and Registration** section from **Voice** > **Ext(n)** and **Survivability Test Mode** parameter under **System Configuration** section from **Voice** > **System**.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 8832 Multiplatform Phones User Guide*
- *XML Reference Guide for Cisco IP Phone Multiplatform Phones*

Upgrade Overview

The upgrade procedure is different according to the current phone firmware version.

- If the current phone firmware is 11.3(1) SR3 or later, see Upgrade the Firmware from a version after 11.3(1) SR3, on page 3.

- If the current phone firmware is 11.3(1) SR2 or earlier, see Upgrade the Firmware from a Version before 11.3(1) SR2, on page 4.

Upgrade the Firmware from a version after 11.3(1) SR3

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

The phone firmware supports the following upgrade paths:

- From 11.3(1) SR3 to 12.0(1)
- From 11.3(2) to 12.0(1)
- From 11.3(3) to 12.0(1)
- From 11.3(4) to 12.0(1)
- From 11.3(5) to 12.0(1)
- From 11.3(6) to 12.0(1)
- From 11.3(7) to 12.0(1)

Procedure

Step 1 Click this link:

https://software.cisco.com/download/home/286311392

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 **IP Conference Phone 8832 with Multiplatform Firmware** 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 **12.0.1** 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 `cmterm-8832.12.0.1MPP0001.245_REL.zip` file.

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>]>/<file
name>.loads
```

Examples:

```
http://10.73.10.223/sip8832.12.0.1MPP0001.245.loads
```

```
https://server.domain.com/sip8832.12.0.1MPP0001.245.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>]/<file
  name>.loads
  ```

  Examples:

  ```
  https://10.74.10.225/admin/upgrade?http://10.73.10.223/sip8832.12.0.1MPP0001.245.loads
  ```

  ```
  https://10.74.10.225/admin/upgrade?https://server.domain.com/firmware/sip8832.12.0.1MPP0001.245.loads
  ```

Note Specify the `<file name>.loads` file in the URL. The `<file name>.zip` file contains other files.

Upgrade the Firmware from a Version before 11.3(1) SR2

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

Before you begin

If the current phone firmware is one of the following versions, you must first upgrade the phone firmware to 11.3(1) SR2.

- 11.2(3)
- 11.2(3) SR1
- 11.3.1
- 11.3(1) SR1

For more information, see Cisco IP Conference Phone 8832 Multiplatform Phones Release Notes for Firmware Release 11.3(1)SR2.

Procedure

Step 1 Click this link:

https://software.cisco.com/download/home/286311392

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 **IP Conference Phone 8832 with Multiplatform Firmware** in the right pane.

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

Step 4 Under **Latest Release**, select **12.0.1**.

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.

`cmterm-8832.12-0-1MPP0001.245_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.

Note If you miss the step to upgrade the phone firmware to **11.3.1 MSR2-6**, then you must place the file under the root directory of the TFTP, HTTP, or HTTPs upgrade server.

Example:

`http://10.73.223/sip8832.12-0-1MPP0001.245_loads`

If the file is placed under a non-root directory of the upgrade server, the upgrade fails.

Example:

`http://10.73.10.223/firmware/sip8832.12-0-1MPP0001.245.loads`

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>]>/<file name>.loads`

    Examples:

    `https://10.73.10.223/sip8832.12-0-1MPP0001.245.loads`

    `https://server.domain.com/sip8832.12-0-1MPP0001.245.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>]/<file
name>.loads
```

Examples:

`https://10.74.10.225/admin/upgrade?http://10.73.10.223/sip8832.sip8832.12-0-1MPP0001.245.loads`

`https://10.74.10.225/admin/upgrade?https://server.domain.com/firmware/sip8832.12-0-1MPP0001.245.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=286319904&rls=12.0(1)&sb=anfr&bt=custV

- To view open caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286319904&rls=12.0(1)&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=286319904&rls=12.0(1)&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 Conference Phone 8832 Multiplatform Phones that use Firmware Release 12.0(1).

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 open at the time this report was compiled. For an updated view of the open defects or to view specific bugs, access the Bug Search Toolkit as described in View Caveats, on page 6.

- CSCvx78045 Add "PoE Power Required" parameter definitions to 8800 MPP administration guide
- CSCvz35920 SSRC changes for outgoing Re-INVITES
- CSCvz67625 License prompt is always displayed on GDS input screen if the phone is converted from On-Premises
- CSCwa70238 MPP should block sending CANCEL when Park button is pressed twice quickly

Resolved Caveats

The following list contains the severity 1, 2, and 3 defects that are resolved for the Cisco IP Conference Phone 8832 Multiplatform Phones that use Firmware Release 12.0(1).

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.

- CSCwa95349 Cloud awareness: Phone will create new registration after reboot or for each refresh request
- CSCwc29314 MPP phones (88xx/68xx/78xx) do not support dual registration with TCP
- CSCwc75949 8832 intermittently mutes and unmutes the microphone without user intervention
- 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

Cisco IP Phone Firmware Support Policy

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