# Cisco IP Conference Phone 8832 Multiplatform Phones Release Notes for Firmware Release 12.0(3)

**First Published:** 2023-08-17

**Last Modified:** 2023-08-17

## Release Notes

Use these release notes with the Cisco IP Conference Phone 8832 Multiplatform Phones running SIP Firmware Release 12.0(3).

The following table describes the individual phone requirements.

| Phone | Support Requirements |
|---|---|
| Cisco IP Conference Phone 8832 Multiplatform Phones | Cisco BroadWorks 24.0<br>MetaSphere CFS version 9.5<br>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

### 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 Conference Phone Multiplatform Phone Administration Guide*

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

## 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 5.

### 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 12.0(2) to 12.0(3)
- From 12.0(1) to 12.0(2)
- 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 **12.0.3** 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-8832.12-0-3MPP0001-87_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/sip8832.12-0-3MPP0001-87.loads
  ```

  ```
  https://server.domain.com/sip8832.12-0-3MPP0001-87.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>]/<file
  name>.loads
  ```

  Examples:

  ```
  https://10.74.10.225/admin/upgrade?http://10.73.10.223/sip8832.12-0-3MPP0001-87.loads
  ```

  ```
  https://10.74.10.225/admin/upgrade?https://server.domain.com/firmware/sip8832.12-0-3MPP0001-87.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** Under **Latest Release**, select **12.0.2**.

**Step 6** (Optional) Place your mouse pointer on the file name to see the file details and checksum values.

**Step 7** Download the corresponding file.

`cmterm-8832.12.0.2MPP0001.116_REL.zip`

**Step 8** Click **Accept License Agreement**.

**Step 9** 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://10.73.10.223/sip8832.12.0.2MPP0001.116.loads
```

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

Example:

```
http://10.73.10.223/sip8832.12.0.2MPP0001.116.loads
```

**Step 10** 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/sip8832.12.0.2MPP0001.116.loads
     ```

     ```
     https://server.domain.com/sip8832.12.0.2MPP0001.116.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:

  ```
  htttps://10.74.10.225/admin/upgrade?http://10.73.10.223/sip8832.sip8832.12.0.2MPP0001.116.loads
  ```

  ```
  https://10.74.10.225/admin/upgrade?https://server.domain.com/firmware/sip8832.12.0.2MPP0001.116.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(3)&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(3)&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(3)&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(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 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 7.

- CSCwf10291—CP-8832-K9= does not support wireless after migration to MPP phone firmware.
- CSCwe55809—Personal contact calls play the distinctive ring while there's an active call on 8800 phones.

## 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(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 7.

- CSCvb65980—Nav hard key can't move cursor in Search Enterprise Directory.
- CSCwa95349—Cloud awareness: Phone will create new registration after reboot or for each refresh request.
- CSCwb65913—ICE: Phone becomes not operational when Media ports are not getting released.
- 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.
- 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.
- CSCwe46272—MPP 12.x not properly optimizing media via ICE on calls to LGW.
- CSCwe67157—Vulnerabilities in linux-kernel - multiple versions CVE-2023-26545.
- CSCwf35777—MPP - 88xx Inbound caller ID issue 12.0.1 Firmware.
- CSCwf82386—Expiring SUDI/MIC in MPP phones.
- CSCwf35777—Inbound caller ID issue.
- CSCwh20086—MPP restarts randomly while idle.

- 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.