Cisco IP Conference Phone 8832 Multiplatform Phones Release Notes for Firmware Release 11.3(5)

First Published: 2021-09-16

Release Notes

Use these release notes with the Cisco IP Conference Phone 8832 Multiplatform Phones running SIP Firmware Release 11.3(5).

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 Features

Keep Focus on the Active Call

You can set up the phone to ensure that the active call is still in focus on the phone screen when the phone receives an incoming call.

To enable this feature, use the **Keep Focus On Active Call** field under the **Supplementary Services** section from **Voice** > **User**.

Where to Find More Information

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

MIC Certificate Renewal by SUDI Service

You can now renew the Manufacture Installed Certificate (MIC) by a Secure Unique Device Identifier (SUDI) renewal service. This is an easy way to provide encryption and to help secure the phone. The MIC certificate involves some features that are related to SSL/TLS protocol. If the MIC certificate expires, these features don't work until you renew the certificate.

When this feature is enabled, the phone automatically renews the MIC certificate. Therefore, there's no additional action required by the user or admin.

To enable this feature, use the parameters under the **MIC Cert Settings** section from **Voice** > **Provisioning**.

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*

Phone Migration without Transition Load

You can now obtain and authorize the licence from the server to migrate your multiplatform phone to enterprise phone firmware in a single step without using transition firmware load. To enable this feature, in the phone web page, use the **Transition Authorization Rule** and **Transition Authorization Type** parameters from **Voice** > **Provisioning** > **Firmware Upgrade**.

Where to Find More Information

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

STIR/SHAKEN Visual Confirmation on the Phones

This release supports new technology standard Secure Telephony Identity Revisited (STIR) and Signature-based Handling of Asserted information using toKENs (SHAKEN). STIR/SHAKEN has been mandated by Federal Communications Commission (FCC). These standards define procedures to authenticate and verify caller identification for calls carried over the IP network. The STIR-SHAKEN framework is developed to provide the end user with a great degree of identification and control over the type of calls they receive. These sets of standards are intended to provide a basis for verifying calls, classifying calls, and facilitating the ability to trust caller identity end to end. Illegitimate callers can easily be identified.

When STIR/SHAKEN support is implemented on the server, the phone displays an extra icon next to the caller ID based on the caller's STIR/SHAKEN verification result. Based on the verification result, the phone displays three types of icons.

Where to Find More Information

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

Support for Dialog-Based Shared Line Appearance

You can now enable dialog-based shared line appearance (SLA) so that the phones in the shared line can subscribe to the dialog event package. This feature supports the following functionalities:

- Incoming call
- Outgoing call
- Public/Private hold and resume
- Barge-in
- Call forward.

To enable this feature, use the **Share Line Event Package Type** parameter from **Voice** > **SIP** > **SIP Parameters** of the phone web interface.

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*

Voicemail Subscription Service Control

You can enable the subscription to a specified voicemail server for an extension. After you configure the voicemail server correctly and enable the subscription to the voicemail server, your user can receive voicemail messages on the phone.

To enable the feature, use the **Voice Mail Enable** field under the **Call Feature Settings** section from **Voice** > **Ext (n)**.

Where to Find More Information

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration 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 4.
- 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 11.3(1) SR3 to 11.3(5)
- From 11.3(2) to 11.3(5)
- From 11.3(3) to 11.3(5)
- From 11.3(4) to 11.3(5)

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 **11.3.5** 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-8832.11-3-5MPP0001-276_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/sip8832.11-3-5MPP0001-276.loads
     ```

     ```
     https://server.domain.com/sip8832.11-3-5MPP0001-276.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/sip8832.11-3-5MPP0001-276.loads`

  `https://10.74.10.225/admin/upgrade?https://server.domain.com/firmware/sip8832.11-3-5MPP0001-276.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 **11.3.5**.

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-8832.11-3-5MPP0001-276_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://10.73.10.223/sip8832.11-3-5MPP0001-276.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/sip8832.11-3-5MPP0001-276.loads`

Step 9 Upgrade the phone firmware with one of these methods.

- Upgrade the phone firmware from the phone administration web page:
  1. **a.** On the phone administration web page, go to **Admin Login** > **Advanced**, **Voice** > **Provisioning** > **Firmware Upgrade**.
  2. **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/sip8832.11-3-5MPP0001-276.loads`

     `https://server.domain.com/sip8832.11-3-5MPP0001-276.loads`

  3. **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/sip8832.11-3-5MPP0001-276.loads

https://10.74.10.225/admin/upgrade?https://server.domain.com/firmware/sip8832.11-3-5MPP0001-276.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=11.3(5)&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=11.3(5)&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=11.3(5)&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 11.3(5).

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.

- CSCvw72979 Phone will show the call center softkey after answer executive or call forward call.
- CSCvx44952 Phone showing Failed to download configurations even when it was successful while migrating to MPP
- CSCvy98097 Set all or part of cfw items to "na" and enable user mode, see the forward sk or cfw item in menu
- CSCvz67625 License prompt is always displayed on the GDS input screen if the phone is converted from On-Prem

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 11.3(5).

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.

- CSCvw69851 CP-8832-3PCC buzzing noise
- CSCvy27737 No reorder tone and will not time out when network conference fail
- CSCvx69154 MPP Not Setting "Don't Fragment" (DF) Bit
- CSCvy36096 Unexpected 481 sent by phone when off/on-hook shared line quickly
- CSCvx44944 Short activation code taking a long time to get configurations
- CSCvs52371 MPP phone call focus on new incoming call

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)

© 2021 Cisco Systems, Inc. All rights reserved.