Cisco IP Conference Phone 7832 Multiplatform Phones Release Notes for Firmware Release 12.0(4)SR1

First Published: 2024-02-27

Release Notes

Use these release notes with the Cisco IP Conference Phone 7832 Multiplatform Phones running SIP Firmware Release 12.0(4)SR1.

The following table describes the individual phone requirements.

Phone	Support Requirements
Cisco IP Conference Phone 7832 Multiplatform Phones	BroadSoft BroadWorks 24.0 MetaSphere CFS version 9.5 Asterisk 13.0

Cisco IP Conference Phone 7832 Documentation

Refer to publications that are specific to your language and call control system. Navigate from the following documentation URL:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-phone-7800-series-multiplatform-firmware/tsd-products-support-series-home.html

New and Changed Features

SRTP Enhancement

Options to enable and disable ROC reset after a re-keying without SSRC/IP/Port changes.

Upgrade the Firmware

The Cisco IP Conference Phone 7832 Multiplatform Phones support a single image upgrade using TFTP, HTTP, or HTTPS protocols with a URL.

After the firmware upgrade completes, the phone reboots automatically.

Procedure

Step 1 Click the following URL:

https://software.cisco.com/download/navigator.html?mdfid=286311381&i=rm

Step 2 Select **IP Phone 7800 Series with Multiplatform Firmware** in the center pane.

Step 3 Select **IP Conference Phone 7832 with Multiplatform Firmware** in the right pane.

Step 4 Select the **Multiplatform Firmware** software type.

Step 5 Under **Latest Release**, select the **12.0.4SR1** folder.

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

Step 7 Download the `cmterm-7832.12-0-4MPP0101-205_REL.zip` file.

Step 8 Click **Accept License Agreement** when you accept the software license.

Step 9 Unzip the firmware files.

Step 10 Put the files in the TFTP, HTTP, or HTTPS download directory.

Step 11 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** tab, **Firmware Upgrade** section. In the **Upgrade Rule** field, enter the load file URL as described below.

  Load file URL format:

  ```
  <upgrade protocol>://<server ip address>[:<port>]>/<path>/<file name>.loads
  ```

  Examples:

  ```
  http://10.73.10.223/firmware/sip7832.12-0-4MPP0101-205.loads
  ```

  ```
  https://server.domain.com/firmware/sip7832.12-0-4MPP0101-205.loads
  ```

  b. 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>://<server ip address>[:<port>]>/<path>/<file name>.loads
  ```

  Example:

  ```
  https://10.74.10.225/admin/upgrade?http://10.73.10.223/firmware/sip7832.12-0-4MPP0101-205.loads
  ```

  ```
  https://10.74.10.225/admin/upgrade?https://server.domain.com/firmware/sip7832.12-0-4MPP0101-205.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

- 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=286319849&rls=12.0(4)&sb=anfr&bt=custV
- To view open caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286319849&rls=12.0(4)&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=286319849&rls=12.0(4)&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 7832 Multiplatform Phones that use Firmware Release 12.0(4)SR1.

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 3.

- CSCwf10956 Macro $SERVIP is not expanded in Log Request Msg in syslog.
- CSCwf70230 78xx is stripping leading "+" when dialling from the monitored line button without extension.
- CSCwi60009 MPP should retry call park resume in race condition scenario with incoming call.

Resolved Caveats

Fix some critical security issue.

Cisco IP Phone Firmware Support Policy

For information on the support policy for phones, see https://cisco.com/go/phonefirmwaresupport.