



Cisco IP Conference Phone 7832 Multiplatform Phones Release Notes for Firmware Release 11.3(6)

First Published: 2022-01-26

Release Notes

Use these release notes with the Cisco IP Conference Phone 7832 Multiplatform Phones running SIP Firmware Release 11.3(6).

The following table describes the individual phone requirements.

Phone	Support Requirements
Cisco IP Conference Phone 7832 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 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

Call Focus Enhancement

The existing feature *Keep Focus on the Active Call* has an enhancement in this release. Now the focus on the phone screen can automatically move to an incoming call if the user places the active call on hold.

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

Where to Find More Information

- *Cisco IP Conference Phone 7832 Multiplatform Phones Administration Guide*
- *XML Reference Guide for Cisco IP Phone Multiplatform Phones*

Enhancements of Displaying Contact Numbers from the LDAP Directory

The phone now separately displays the LDAP user's contact numbers in the contact details screen. As a user, you can select one of the contact numbers before you edit the number or directly make a call.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Multiplatform Phones User Guide*

Enhancements of Displaying Contact Numbers from the XML Directory

The phone now displays the contact numbers of a XML address entry separately on the phone screen. As a user, you can do the following activities:

- View the details of an XML address entry
- Select a specific contact number to dial out by viewing the details of an XML address entry
- Dial out the first contact number of an XML address entry

Where to Find More Information

- *Cisco IP Conference Phone 7832 Multiplatform Phones User Guide*

Permission Only for the Call Forward All Service Setup

You can configure the phone to allow the user directly set up the Call Forward All service by pressing the **Forward all** softkey. By default, the user can set up all call forward services, including Call Forward All, Call Forward Busy, and Call Forward No Answer by the **Forward** softkey.

To enable this feature, use the **Forward Softkey** parameter under the **Call Forward** section from **Voice > User** on the phone web interface,.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Multiplatform Phones Administration Guide*
- *XML Reference Guide for Cisco IP Phone Multiplatform Phones*

PRT Generation of Multiplatform Phones from the Webex Control Hub

You can now generate a problem report of a phone from the Webex Control Hub if the phone successfully onboards to Webex cloud.

After you generate a problem report, check the PRT upload information on the phone from a new phone menu, **Last problem report info**. On the phone administration web page, from **Info > Status > PRT Status**, you can see that the upload information is triggered from the Webex Control Hub.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Series Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 7832 Series Multiplatform Phones User Guide*
- *Webex for Cisco BroadWorks Solution Guide*

Reboot of Multiplatform Phones from the Webex Control Hub

You can reboot phone remotely from the Webex Control Hub. The phone must onboard to Webex cloud if you want to reboot it remotely. You can only reboot a phone that is in idle state. If the phone is in use, such as in a call, the phone doesn't reboot.

After successful reboot, check the status on the phone administration web page from **Info > Status > Reboot History**. The **Reboot Reason** parameter under **Reboot History** shows the reboot reason as **Cloud Triggerred**. You can also check the reboot reason as **Cloud triggered** on the phone from **Application > Status > Reboot history**.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Series Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 7832 Series Multiplatform Phones User Guide*
- *Webex for Cisco BroadWorks Solution Guide*

Support for French (Canada) Language

Phone now supports French (Canada) language. All multiplatform IP phones and all key expansion modules (KEM) now support the language.

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

Where to Find More Information

- *Cisco IP Conference Phone 7832 Series Multiplatform Phones Administration Guide*

Webex Cloud Onboarding of Multiplatform Phones

You can onboard a phone to Webex cloud either with activation code onboarding (GDS) or with phone MAC address (EDOS device activation). When the phone onboards to Webex cloud, you can reboot the phone and can also generate a problem report from the Webex Control Hub.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Series Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 7832 Series Multiplatform Phones User Guide*

- *Webex for Cisco BroadWorks Solution Guide*

Upgrade the Firmware

Use the information in this section to upgrade the firmware on Cisco IP Conference Phone 7832 Multiplatform Phones.

The Cisco IP Phone 7811, 7821, 7841, and 7861 Multiplatform Phones have a different firmware image. For more information, see the Cisco IP Phone 7800 Series Multiplatform Phones Release Notes for Firmware Release 11.3(6), at this location:

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-phone-7800-series-multiplatform-firmware/products-release-notes-list.html>

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/286311381>
- On the **Software Download** web page that is displayed, ensure that **IP Phone 7800 Series with Multiplatform Firmware** is selected in the middle pane.
- Step 2** Select **IP Conference Phone 7832 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 **11.3.6** 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-7832.11-3-6MPP0001-273_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>]/<path>/<file name>.loads
```

 Example:

```
https://10.73.10.223/firmware/sip7832.11-3-6MPP0001-273.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
```

Example:

```
https://10.74.10.225/admin/upgrade?https://10.73.10.223/firmware/sip7832.11-3-6MPP0001-273.loads
```

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

Limitations and Restrictions

Backward Compatibility of Password

Since Firmware Release 11.3(6) introduces a mechanism to enhance the security, certain passwords don't support back-compatibility.

This behaviour only affects the passwords that are updated in the 11.3(6).

For more information, refer to the *Saved Passwords Become Invalid after Downgrade* section in the following guide:

- *Cisco IP Conference Phone 7832 Multiplatform Phones Administration Guide*

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=286319849&rls=11.3\(6\)&sb=anfr&bt=custV](https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=286319849&rls=11.3(6)&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=11.3\(6\)&sb=anfr&sts=open&bt=custV](https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=286319849&rls=11.3(6)&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=11.3\(6\)&sb=anfr&sts=fd&bt=custV](https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=286319849&rls=11.3(6)&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 (*CSCxxxxnnnnn*) 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 11.3(6).

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 (*CSCxxxxnnnnn*). 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 5](#).

- 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
- 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 7832 Multiplatform Phones that use Firmware Release 11.3(6).

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 (*CSCxxxxnnnnn*). 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](#).

- CSCvu62280 Multiple Vulnerabilities in glibc
- CSCvx84320 Evaluation of 78xx for OpenSSL March 2021 vulnerabilities
- CSCwa05021 MPP 78xx does not show Japanese character "さ" (unicode U+3055 Hiragana) properly
- CSCvy98097 Set all or part of cfw items to "na" and enable user mode, see the forward sk or cfw item in menu

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)

© 2022 Cisco Systems, Inc. All rights reserved.