Cisco IP Conference Phone 7832 Multiplatform Phones Release Notes for Firmware Release 11.2(3)

First Published: 2019-01-30

Release Notes

Use these release notes with the Cisco IP Conference Phone 7832 Multiplatform Phones running SIP Firmware Release 11.2(3).

The following table describes the individual phone requirements.

Phone	Support Server
Cisco IP Conference Phone 7832 Multiplatform Phones	BroadSoft BroadWorks 22.0 MetaSphere CFS version 9.4 Asterisk 11.0

Related Documentation

Use the following sections to obtain related information.

Cisco IP Conference Phone 7832 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-7800-series-multiplatform-firmware/index.html

New and Changed Features

Catalan Language Support

You and your user can set the phones to display text in Catalan. On the phone administration web page, the **Locale** field in **Voice** > **Regional** contains the new **ca-ES** option.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Multiplatform Phones Administration Guide*
- *Cisco IP Phone 7800 Series Multiplatform Phones Provisioning Guide*

Control of Phone Configuration Reporting

You can control when the phone reports its configuration to the provisioning server. This is in addition to the standard report upload that happens as part of the phone shutdown or restart.

Use the new **Report to Server** drop-down list on the phone administration web page, in **Voice** > **Provisioning** > **Upload Configuration Options**. When you choose **On Local Change**, the phone reports its configuration when any configuration parameter changes by an action on the phone or on the phone administration web page. The phone waits for a few seconds after a change is made, and then reports the configuration. This wait time is defined in the **Upload Delay On Local Change** field. Specify a value in number of seconds (10 minimum, 60 default, 900 maximum). This delay ensures that changes are reported to the web server in batches, rather than reporting a single change at a time.

Alternately, the phone can report its configuration at regular intervals. Choose **Periodically** in the **Report to Server** drop-down list. Then, in the **Periodic Upload to Server** field, specify an interval in number of seconds (600 minimum, 3600 default, 2592000 (30 days) maximum).

In all cases, the report rule that you specify defines the configuration report that the phone sends. Two report upload destination URLs are supported in the **Report Rule** field which provide flexibility in both destination and content of the uploaded report.

This feature has no user impact.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Multiplatform Phones Administration Guide*
- *Cisco IP Phone 7800 Series Multiplatform Phones Provisioning Guide*

Device Identifier in Uploaded Syslog Messages

You can now choose to include a device identifier for the phone in syslog messages that are uploaded to the syslog server. While the IP address of a phone may change over time, the device identifier does not change. This can ease the process of identifying the source of each message in a stream of incoming messages from multiple phones. The device identifier appears after the timestamp in each message.

On the phone administration web page, you will see a new field named **Syslog Identifier** in **Voice** > **System** > **Optional Network Configuration**. You can also configure this setting in the XML configuration file. You can choose the type of device identifier to include:

- none
- the MAC address of the phone, in the standard colon-separated format, or as continuous upper case or lower case letters and digits
- the product serial number of the phone

This feature has no user impact.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Multiplatform Phones Administration Guide*
- *Cisco IP Phone 7800 Series Multiplatform Phones Provisioning Guide*

DND and Call Forwarding Sync Between the Phone and the Server

Besides Feature Key Synchronization (FKS), you can also enable the do not disturb (DND) and call forwarding synchronization between the phone and the server through the XSI service. When both FKS and XSI Synchronization are enabled, FKS takes precedent over XSI Synchronization.

You use the new fields **DND Enable** and **CFWD Enable** on the phone administration web page to enable or disable this feature. When enabled, the settings of DND and call forwarding on the server are synchronized to the phone. The status changes made on the phone will also be synchronized to the server.

The fields are located in the **XSI Line Service** section from **Voice** > **Ext (n)**.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Multiplatform Phones Administration Guide*
- *Cisco IP Phone 7800 Series Multiplatform Phones Provisioning Guide*

Profile Account Authentication

Profile account authentication enables the phone to resynchronize the provisioning profile. You can specify a profile authentication type for phone users to use.

The new field **Profile Authentication Type** replaces the **Profile Account Enable** field on the phone administration web page. The available options are: Disabled, Basic HTTP Authentication, and XSI Authentication.

When you disable this feature, the phone user can't enter the authentication account on the phone screen. When you specify an authentication type, the phone user can use the provided credentials to resynchronize the provisioning profile either when prompted or through the **Profile account setup** menu on the phone screen.

If **XSI Authentication** is specified as the authentication type, you can use either XSI login credentials or SIP credentials to resynchronize the provisioning profile. Logging into XSI server with SIP credentials requires Broadsoft Broadworks 20.0 or later versions.

To use SIP credentials, set **XSI Host Server**, **XSI Authentication Type** (as **SIP Credentials**), **SIP Auth ID**, and **SIP Password** in the **XSI Phone Service** section from the **Voice** > **Phone** tab on the phone administration web page.

Where to Find More Information

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

RFC 8188-Based HTTP Content Encryption for Configuration Files

The phone now supports RFC 8188-based HTTP content encryption with AES-128-GCM ciphering for configuration files. With this encryption method, any entity can read the HTTP message headers. However, only the entities that know the Input Keying Material (IKM) can read the payload. When the phone is provisioned with the IKM, the phone and the provisioning server can exchange configuration files securely, while allowing third-party network elements to use the message headers for analytic and monitoring purposes.

The new XML configuration parameter **`IKM_HTTP_Encrypt_Content`** holds the IKM on the phone. For security reasons, this parameter is not accessible on the phone administration web page. It is also not visible in the phone's configuration file, which you can access from the phone's IP address or from the phone's configuration reports sent to the provisioning server.

Note The phone continues to support the AES-256-CBC encryption method. As in the previous release, you specify the AES-256-CBC key with the **`--key`** keyword in profile rules and report rules. Which of the two encryption and decryption methods the phone applies depends on the inputs that you provide.

If you want to use the RFC 8188-based encryption, ensure the following:

- Provision the phone with the IKM by specifying the IKM with the new XML parameter **`IKM_HTTP_Encrypt_Content`** in the configuration file that is sent from the provisioning server to the phone.
- If this encryption is applied to the configuration files sent from the provisioning server to the phone, ensure that the *Content-Encoding* HTTP header in the configuration file has "aes128gcm".

  In the absence of this header, the AES-256-CBC method is given precedence. The phone applies AES-256-CBC decryption if a AES-256-CBC key is present in a profile rule, regardless of IKM.
- If you want the phone to apply this encryption to the configuration reports that it sends to the provisioning server, ensure that there is no AES-256-CBC key specified in the report rule.

This feature has no user impact.

Where to Find More Information

- *Cisco IP Phone 7800 Series Multiplatform Phones Provisioning Guide*
- *Cisco IP Conference Phone 7832 Multiplatform Phones Administration Guide*

Remotely Initiated Problem Reports

You can initiate a phone problem report remotely. To do this, initiate a `SIP-NOTIFY` message from the server to the phone, with the Event specified as `prt-gen`. The phone generates a problem report using the Cisco Problem Report Tool (PRT), with the problem description "Remote PRT Trigger". If you have configured an upload rule for problem reports, the phone also uploads the problem report according to the upload rule.

You can see the status of the most recent problem report initiation on the phone administration web page > **Info** > **Status**. A new section called **PRT Status** shows the location of initiation and the status of the report generation, and the status of the report upload.

You can access a remotely-initiated problem report from the same location as locally-initiated problem reports on the phone administration web page.

This feature has no user impact.

Where to Find More Information

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

Support for Early Media and Preconditions

Your phone now supports early media negotiation and precondition signaling.

For an outgoing call, a SIP message from the phone includes the P-Early-Media header, which contains the status of the early media stream. If the status in the header is not indicating that the network is blocking the early media stream, the phone plays the early media instead of the ringback tone while waiting for the call to be connected.

Precondition signaling defers incoming call notifications until the phone receives the message that preconditions are satisfied to establish the call.

Where to Find More Information

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

Contact Search in Multiple Directories

You can now search for contacts by name in multiple directories simultaneously. The new **All** menu item in the **Directories** menu provides this function. The phone searches for the name in the following locations if Broadsoft directories are configured:

- All Broadsoft directories
    - Enterprise directory
    - Group directory (included in the Enterprise directory)
    - Enterprise Common directory
    - Group Common directory
    - Personal directory
- The LDAP directory, if configured
- The personal address book on the phone

The search function behaves in a similar manner to the name-search function within individual directories. The search results show both full and partial name matches. You can select a contact in the search results and then view contact details, add the contact to the personal address book, and call the contact. You can also edit the number before making the call.

Where to Find More Information

- *Cisco IP Conference Phone 7832 Multiplatform Phones User Guide*
- *Cisco IP Conference Phone 7832 Multiplatform Phones Administration 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 11.2(3), 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 **11.2.3** 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-7832.11-2-3MPP-398_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:

  1. On the phone administration web page, go to **Admin Login** > **Advanced**, **Voice** > **Provisioning** > **Firmware Upgrade**.

  2. 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/sip7832.11-2-3MPP-398.loads
     ```

  3. 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/sip7832.11-2-3MPP-398.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

Caller Identification and Other Phone Functions

Caller identification or other phone functions have not been verified with third-party applications for the visually or hearing impaired.

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=11.2(3)&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=11.2(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=286319849&rls=11.2(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 7832 Multiplatform Phones that use Firmware Release 11.2(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.

- CSCvo01547 When phone set ignore incoming call , current ringer volume is not right

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 11.2(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.

- CSCvm70118 From missed call screen there is no way to go back
- CSCvm04591 When two phones are in a dial-up connection, there is no call status in the Web GUI
- CSCvm95087 Syslog is missing bootup logs and PRT is missing older log archives

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.