Cisco IP Conference Phone 8832 Multiplatform Phones Release Notes for Firmware Release 11.3(1)

First Published: 2019-11-19

Release Notes

Use these release notes with the Cisco IP Conference Phone 8832 Multiplatform Phones running SIP Firmware Release 11.3(1).

The following table describes the individual phone requirements.

Phone	Support Requirements
Cisco IP Conference Phone 8832 Multiplatform Phones	BroadSoft BroadWorks 22.0 MetaSphere CFS version 9.5 Asterisk 11.0

Related Documents

The following sections describe the documentation enhancement and additional documentation information.

Documentation Enhancement

Starting with Firmware Release 11.3(1), the Administration Guide is enhanced by integrating the information from the previous Provisioning Guide. The enhanced Administration Guide describes how to configure the phones with either the configuration file or the phone web interface.

Two additional guides are added: *FAQ for Cisco IP Phones with Multiplatform Firmware* and *BroadSoft Quick Start Guide*.

The complete documentation suite is:

- *Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide*
- *Cisco IP Conference Phone 8832 Multiplatform Phones User Guide*
- *Cisco IP Conference Phone 8832 Multiplatform Phones Release Notes*
- *FAQ for Cisco IP Phones with Multiplatform Firmware*
- *BroadSoft Quick Start Guide* (for BroadSoft platform only)

Cisco IP Phone 8832 Series 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

Cipher Configuration

You can specify the cipher suites that the phone TLS applications use. This feature lets you select which TLS cipher suites are enabled or disabled on the phone.

To specify the cipher suites, use the **TLS Cipher List** field on the **Voice** > **System** tab of the phone administration web page. The cipher list consists of one or multiple cipher suites. For multiple cipher suites, the suites are colon-delimited. When you specify a valid cipher list, the list applies to all the TLS applications on the phone. A valid cipher list must follow a specific format. For the cipher list formats, see https://www.openssl.org/docs/man1.0.2/man1/ciphers.html.

By default, no cipher list is specified in this field. The system regards an invalid list as a blank value. With a blank or an invalid list in this field, the cipher suites used vary with applications.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

DNS SRV for HTTP Provisioning

You can enable auto provisioning of your multiplatform phones with this feature. Domain Name System Service (DNS SRV) records establish connections between a service and a hostname. When the phone looks for the location of the provisioning service, it first queries on the given DNS SRV domain name, then it queries for SRV records. The phone validates the records to confirm that the server is accessible. Then, it continues to the actual provisioning flow. Service providers can utilize this DNS SRV provisioning flow to provide auto provisioning.

DNS SRV bases the hostname validation on the certificate of the DHCP provided domain name. It's important that all SRV records use a valid certificate containing the DHCP provided domain name.

The DNS SRV query includes the DHCP domain name in its construction as follows: **`_<servicename>._<transport>.<domainName>`**.

For example, **`_ciscoprov-https._tls.example.com`**, instructs the phone to do a lookup for `example.com`. The phone uses the hostname and port number that is retrieved from DNS SRV query to build the URL and download the initial configuration from it.

DNS SRV is one of many auto provisioning mechanisms that the phone uses. The phone tries the mechanisms in the following order:

1. DHCP
2. DNS SRV
3. EDOS
4. GDS (Activation Code Onboarding), or EDOS Device Activation

DNS SRV doesn't support the TFTP protocol. If you use TFTP, you receive the following error message: `Error - TFTP Scheme not supported in SRV lookups.`

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

DTMF RFC4733 Support

Your phones now support RFC4733. You can choose from three audio-video transport (AVT) options for sending DTMF pulses to the server.

- *AVT Dynamic Payload* for 8 kHz clock rate
- *AVT 16kHz Dynamic Payload* for 16 kHz clock rate
- *AVT 48kHz Dynamic Payload* for 48 kHz clock rate

Configured dynamic payloads are used for outbound calls only when the phone presents a Session Description Protocol (SDP) offer.

You can configure the **AVT Dynamic Payload** options in the **SDP Payload** section of the phone web page.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

Auto Provisioning with Short Activation Code

You can provide users with an activation code to set up their phones with this feature. Users enter the short activation code on the phone Welcome screen. Then, the phone receives its provisioning information.

This feature uses the cloud provisioning method via the CDA (EDOS) server. It doesn't require MAC addresses added to the CDA server.

The short activation code has any number of digits between 3 and 16, inclusive. Users press pound (#), then enter the short code digits. Use this format: **#nnn**, **#nnnnnnnnnnnnnnnn**, or any number of digits between 3 and 16. The pound (#) key signals that the user is attempting to use Auto Provisioning with Short Activation Code. Otherwise, the phone expects the 16-digit code for the Activation Code Onboarding feature. If the user fails to enter pound (#) before the digits, the phone displays `Invalid activation code`. The same message displays if the user enters any wrong code.

If the phone fails to register with the correct code, reset the phone to the factory settings, and try again.

Where to Find More Information

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

End-of-Call Statistics on Media Session Changes (BYE and re-INVITE)

You can enable the phone to send end-of-call statistics in Session Initiation Protocol (SIP) messages. The phone sends call statistics to a remote end when a call terminates or when a call is on hold. The call statistics are sent as headers in BYE and re-INVITE messages: `RTP-RxStat` and `RTP-TxStat` for audio sessions.

By default, the phone doesn't send call statistics. You can enable this feature using the **Call Statistics** field on the **Voice** > **SIP** tab of the phone administration web page.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

Hostname Verification over TLS

You can enable increased phone security on a phone line if you use TLS. The phone line can verify the hostname to determine if the connection is secure.

Over a TLS connection, the phone can verify the hostname to check the server identity. The phone can check both the Subject Alternative Name (SAN) and the Subject Common Name (CN). If the hostname on the valid certificate matches the hostname that is used to communicate with the server, the TLS connection establishes. Otherwise, the TLS connection fails.

The phone always verifies the hostname for the following applications:

- LDAPS
- XMPP
- Image upgrade over HTTPS
- XSI over HTTPS
- File download over HTTPS
- TR-069

When a phone line transports SIP messages over TLS, you can control the hostname verification with the **TLS Name Validate** field on the **Ext(n)** tab. Set the field to **Yes** to verify the hostname. Set the field to **No** to bypass the hostname verification.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

Support for Client-Initiated Media Plane Security Negotiation

You can choose client-initiated mode or server-initiated mode for media plane security negotiations between the phone and the server. Set the **MediaSec Request** field to **Yes** to enable the phone to initiate negotiations with the server for media plane security. The default setting is **No** (server-initiated mode). The security mechanism follows the standards stated in RFC 3329 and its extension draft *Security Mechanism Names for Media* (See https://tools.ietf.org/html/draft-dawes-sipcore-mediasec-parameter-08#ref-2). You can use the **MediaSec Over TLS Only** field to limit that media plane security negotiation is applied only when SIP signaling transport protocol is TLS.

Access the parameters in the **SIP Settings** section on the **Voice** > **Ext (n)** tab of the phone web interface.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

On-Device Firewall

We have improved phone security by hardening the operating system. Hardening ensures that the phone has a firewall to protect it from malicious incoming traffic.

The firewall tracks the ports for incoming and outgoing data. It detects incoming traffic from unexpected sources and blocks the access. The firewall allows all outgoing traffic.

The firewall is enabled by default, and is configured with the default open UDP and TCP ports. You can change the setting from the **Voice** > **System** > **Security Settings** > **Firewall** section of the phone web page. Firewall changes don't require the phone to reset. Phone soft restarts generally don't affect firewall operation.

You can also control other firewall options with keywords. For more information, see the administration guide.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

Multicast Paging

You can set up multicast paging to allow the users to page to phones. The page can go to all phones or a group of phones in the same network. Any phone in the group can initiate a multicast paging session. Only the phones that listen for the paging group can receive the page.

You can add a phone to a maximum of ten paging groups. Each paging group has a unique multicast port and number. The phones within a paging group must subscribe to the same multicast IP address, port, and multicast number.

You can configure the priority for the page from a specific group. When a phone is active and a page session with a higher priority occurs, the user hears the page on the active audio path. Configure the priority on the **Voice** > **Phone** tab of the administration web page.

When multiple paging sessions occur, the phone answers them in chronological order. The phone doesn't answer the next page until the active page ends. When do not disturb (DND) is enabled, the phone ignores incoming paging.

You can specify a codec for the paging to use. The supported codecs are G711a, G711u, G722, and G729. If you don't specify the codec, paging uses G711u by default.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

OPUS Codec Narrowband

The multiplatform phones now support OPUS Codec Narrowband. The OPUS Codec Narrowband saves on network bandwidth. The multiplatform phones support OPUS codec, and as of Firmware Release 11.3(1), you can configure the phone to use both wideband and narrowband. The phones can use the OPUS narrowband and wideband codecs without conflict.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

PSK with DTMF Support

You can configure programmable softkeys (PSK) with dual tone multifrequency (DTMF). This configuration enables the phone to send digital pulses to the server during an active call. When you enable a function on a PSK, the user sees the softkey name, and presses it to perform the named function.

This feature applies only to programmable softkeys. It doesn't apply to programmable line keys (PLK). If you configure any PLK for this feature, the display presents the Circled X icon ⊗, and nothing happens when you press the key.

This feature supports only **Connected Key List** and **Connected Video Key List**.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

Remote SDK

The phones now support the remote software development kit (SDK). The remote SDK provides a WebSocket-based protocol to control the phones. The remote SDK uses a WebSocket connection, initiated by the phone, to allow the controlling WebSocket server to send commands, receive command results, and events from the phone.

You can configure the remote SDK from the phone web interface in **Voice** > **Phone** > **WebSocket API**.

This feature is supported on Firmware Release 11.3(1) and later.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

SIP and Media Transmission Optimization

You can configure your phone to start an RTP session either before or after the phone receives an ACK from the calling party. This configuration optimizes the media transmission in an environment that experiences audio losses caused by the ACK transmission delay.

Use the **RTP Before ACK** field on the **Voice** > **SIP** tab of the phone administration web page. When set to **Yes**, the RTP transmission doesn't await an ACK, but starts after a 200 OK message is sent out. When set to **No**, the RTP transmission doesn't start until an ACK is received. The default setting is **No**.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

SIP Session-ID Support

The phones now support "Session Identifier". This feature helps to overcome the limitations with the existing call-identifiers and allows end-to-end tracking of a SIP session in IP-based multimedia communication systems in compliance with RFC 7989. To support session identifier, "Session-ID" header is added in the SIP request and response messages.

You can enable this feature from **Voice** > **Ext(n)** > **SIP Settings** > **SIP SessionID Supports** in the phone web interface.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

Serviceability Enhancement Messages

Your phone provides enhanced serviceability messages immediately after it boots up and has invalid provisioning settings. The enhancement provides valuable information that would otherwise be difficult to obtain.

If the provisioning settings are invalid, the phone displays the message `Verify your provisioning settings or contact your service provider.` You can get more information from a softkey. This message displays only when the phone boots up and can't register to the call server. It doesn't display if your administrator inadvertently attempts to apply invalid provisioning settings after the phone has registered.

You don't see the messages when the problem is resolved. You can view the messages under **Settings** > **Status** > **Status Message** on the phone screen.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones User Guide

UDI Display

The phones display the complete Unique Device Identifier (UDI) information on the phone screen and on the phone web page. Cisco UDI provides a unique identity for all Cisco hardware products on which it has been enabled. The UDI is composed of three data elements associated with the phone. The data elements are:

- Product Identifier (PID)
- Version Identifier (VID)
- Serial Number (SN)

To view the UID information, do one of the following:

- On your phone, select **Settings** > **Status** > **Product information**
- In the phone web interface, select **Info** > **Status** >**Product Information**.

Where to Find More Information

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

VQM SIP Publish Message New Field

You can assign a name to your Voice Quality Metrics (VQM) SIP Publish Message report. The name helps you organize your voice quality reports.

You add your report name in the **Voice Quality Report Group** field on the **Voice** > **Ext(n)** tab of the phone web page. Your report name can't begin with a hyphen (-), semicolon (;), or a space.

You can also configure the **Voice Quality Report Group** field in the XML configuration file.

You can look up your report in a packet analyzer, such as, Wireshark. In the packet analyzer, the **Voice Quality Report Group** field appears as **LocalGroup**.

Where to Find More Information

Cisco IP Conference Phone 8832 Multiplatform Phones Administration Guide

Upgrade the Firmware

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/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 your phone model 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 **11.3.1** 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 firmware file: `cmterm-8832.11-3-1MPP-697_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.

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/sip8832.11-3-1MPP-697.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/sip8832.11-3-1MPP-697.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 using the Cisco Bug Search tool.

Known caveats (bugs) are graded according to severity level, and are either open or resolved.

Before you begin

To view the caveats, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Procedure

Step 1 Perform one of the following actions:

- To find all caveats, use this URL:

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311392&sb=anfr&bt=custV

- To find all open caveats, use this URL:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311392&sb=anfr&sts=open&bt=custV
- To find all resolved caveats, use this URL:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311392&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 caveats that are open for the Cisco IP Conference Phone 8832 Multiplatform Phones that use Firmware Release 11.3(1).

This list reflects a snapshot of the caveats that were open at the time this report was compiled. The status of caveats may have changed since then. For an updated view of the resolved caveats, or to view details or history for specific caveats, access the Bug Search Toolkit as described in View Caveats, on page 9. You must be a registered Cisco.com user to access this information.

- CSCvr86301 Remote SDK: WebSocket Control Server URL waits 10 seconds after HTTP 401 Challenge
- CSCvr86286 Remote SDK: WebSocket Control Server URL field does not honor HTTP/1.0 Redirects
- CSCvo26146 Enable/Disable Vertical Service Activation Codes toggle button addition
- CSCvr38502 Profile account setup toast does not work with provisioning on LCD
- CSCvr90430 7832 8832 LED status is incorrectly displayed on web page

Resolved Caveats

The following list contains the severity 1, 2, and 3 caveats that are resolved for the Cisco IP Conference Phone 8832 Multiplatform Phones that use Firmware Release 11.3(1).

This list reflects a snapshot of the caveats that were resolved at the time this report was compiled. The status of caveats may have changed since then. For an updated view of the resolved caveats, or to view details or history for specific caveats, access the Bug Search Toolkit as described in View Caveats, on page 9. You must be a registered Cisco.com user to access this information.

- CSCvq23761 Evaluation of 8832 for TCP SACK vulnerabilities
- CSCvq98680 CP-88xx Phone reboots and not being logged
- CSCvq96403 libjpeg and libjpeg-turbo get_sos Function Information Disclosure Vu ...
- CSCvq57995 Focus not returning to primary line after shared appearance active
- CSCvq71940 Phones restart with XSI directory usage for large enterprises
- CSCvq58001 Phone 'ACK' does not have 'Route' header

- CSCvq96777 Multiple Vulnerabilities in FreeType
- CSCvr17942 Multiple Vulnerabilities in linux_kernel
- CSCvq29665 PRT log description shows MAC as Serial Number
- CSCvo43984 CP-88xx, TR-069 issue
- CSCvp16819 No Answer Delay Ring Count updated incorrectly
- CSCvq48914 Call Recoding Fails to Start (o - line not incrementing in SDP)
- CSCvo46210 Phones have only 25 BLF entries
- CSCvq00877 Resume Recording Failed-OwnerCreator Session ID Not Incrementing in SDP
- CSCvq63855 Call History shows unexpected number when Call-Info/PAID has different CLID
- CSCvr14573 Multiple Vulnerabilities in linux_kernel
- CSCvr37015 Phone does not return to main SIP proxy after the connection has been restored
- CSCvr61497 Upgrade libpcap to 1.9.1 and tcpdump to 4.9.3
- CSCvr58188 Multiple Vulnerabilities in linux_kernel
- CSCvr67580 Multiple Vulnerabilities in linux_kernel
- CSCvr48050 Lib: cURL and libcurl tftp_receive_packet() Function Heap Buffer Overflow …
- CSCvq50638 Phones Meet me conference no audio
- CSCvp53228 Phones do not change media codec after codec negotiation during call
- CSCvs02868 1-way audio on OPUS codec if remote does not send OPUS codec fmt

Cisco IP Phone Firmware Support Policy

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