Cisco IP Phone 8800 Series Release Notes for Firmware Release 11.0(1)

First Published: 2015-11-25

Last Modified: 2017-02-28

Cisco IP Phone 8800 Series Release Notes for Firmware Release 11.0(1)

These release notes support the Cisco IP Phone 8811, 8841, 8845, 8851, 8851NR, 8861, and 8865 running SIP Firmware Release 11.0(1).

Media Port Range has been restricted to UDP/16384-49151. The range 49152-53247 is reserved for ephemeral ports, while 53248-65536 is reserved for VPN use. This is a change from earlier firmware versions, which allowed a Media Port Range from 16384 to 65536.

The following table lists the support and protocol compatibility for the Cisco IP Phones.

Table 1: Cisco IP Phones, Support, and Firmware Release Compatibility

Cisco IP Phone	Protocol	Support Requirements
8811, 8841, 8845, 8851, 8851NR, 8861, and 8865	SIP	Cisco Unified Communications Manager 8.5(1) and later Cisco Unified Communications Manager DST Olsen version D or later SRST 8.0 (IOS load 15.1(1)T) and above Cisco Expressway 8.7
8811, 8841, 8851, 8851NR, and 8861	SIP	CME 10.0

Related Documentation

Use the following sections to obtain related information.

Cisco IP Phone 8800 Series Documentation

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

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/tsd-products-support-series-home.html

The Deployment Guide is located at the following URL:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

Cisco Unified Communications Manager Documentation

See the *Cisco Unified Communications Manager Documentation Guide* and other publications that are specific to your Cisco Unified Communications Manager release. Navigate from the following documentation URL:

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

New and Changed Features

Features Available with the Firmware Release

The following sections describe the features available with the Firmware Release.

Application Dial Rules

Application Dial Rules can now be used to strip numbers from or add numbers to your Bluetooth contact phone numbers. When the administrator enables Application Dial Rules, users can import and dial their Bluetooth contacts without having to modify the contact's phone numbers.

Application Dial Rules only applies to Bluetooth imported contacts and not to the core Cisco Unified Communications Manager Dial Plan. For situations not involving Bluetooth imported contacts, Cisco Unified Communications Manager translation or transformation patterns should be used to modify the core dial plan.

This feature is supported on the following phones:

- Cisco IP Phone 8845
- Cisco IP Phone 8851
- Cisco IP Phone 8861
- Cisco IP Phone 8865

Where to Find More Information

- *Cisco IP Phone 8800 Series Administration Guide*

Audio Voicemail Access from Visual Voicemail

Users can access their audio voicemail from the Visual Voicemail sign-in window. This feature is useful if they want to listen to their voicemail messages, but they don't want to read their list of messages.

This feature is supported on the following phones:

- Cisco IP Phone 8811
- Cisco IP Phone 8841
- Cisco IP Phone 8845
- Cisco IP Phone 8851
- Cisco IP Phone 8851NR
- Cisco IP Phone 8861
- Cisco IP Phone 8865

Where to Find More Information

- *Cisco IP Phone 8800 Series Administration Guide*
- *Cisco IP Phone 8800 Series User Guide*

Barge Enhancements for Cisco IP Phone 8800 Series

With this feature, users without an external media bridge for cBarg can now join an active call or monitor a call using the phone's built-in bridge.

This enhancement gives administrators a choice between deploying Barge and cBarge for users with a built-in bridge. The Barge softkey is displayed on the phone regardless of whether Barge or cBarge is enabled.

This feature is supported on the following phones:

- Cisco IP Phone 8811
- Cisco IP Phone 8841
- Cisco IP Phone 8845
- Cisco IP Phone 8851
- Cisco IP Phone 8851NR
- Cisco IP Phone 8861
- Cisco IP Phone 8865

Where to Find More Information

- *Cisco IP Phone 8800 Series Administration Guide*
- *Cisco IP Phone 8800 Series User Guide*

Enhanced Debugging Options

The Enhanced Debugging Options feature introduces more debugging options for the Cisco IP Phone. When administrators experience phone problem that they cannot resolve, they can enable debugging for the phone, reproduce the problem, and send the logs to Cisco TAC for analysis. Administrators can also implement multilevel and multisection support of the parameters. The debugging options that administrators can select for logs are:

- Preset (default)
- Default
- Telephony
- SIP
- UI
- Network
- Media
- Upgrade
- Accessory
- Security
- Wi-Fi
- VPN
- Energywise
- MobileRemoteAccess

This feature is supported on the following phones:

- Cisco IP Phone 8811
- Cisco IP Phone 8841
- Cisco IP Phone 8845
- Cisco IP Phone 8851
- Cisco IP Phone 8851NR
- Cisco IP Phone 8861
- Cisco IP Phone 8865

Where to Find More Information

- *Cisco IP Phone 8800 Series Administration Guide*
- *Cisco IP Phone 8800 Series User Guide*

Mobile and Remote Access Through Expressway

Mobile and Remote Access through Expressway(MRA) is now officially supported.

In addition, users with a video phone can now scan a QR code to sign into MRA, instead of manually entering the service domain and username. The QR code contains either the service domain, or the service domain and username separated by a comma. For example: mra.example.com or mra.example.com,username.

MRA provides a way for remote workers to easily and securely connect into the corporate network without using a virtual private network (VPN) client tunnel. The feature uses Transport Layer Security (TLS) to secure network traffic.

MRA is supported by:

- Cisco Unified Communications Manager: 10.5(2) and above
- Cisco Expressay: 8.7 and above.

MRA is supported on the following phones:

- Cisco IP Phone 8811
- Cisco IP Phone 8841
- Cisco IP Phone 8845
- Cisco IP Phone 8851
- Cisco IP Phone 8851NR
- Cisco IP Phone 8861
- Cisco IP Phone 8865

Where to Find More Information

- *Cisco IP Phone 8800 Series Administration Guide*
- *Cisco IP Phone 8800 Series User Guide*

Problem Report Tool

On-premise users can submit problem reports to their administrator with the Problem Report Tool.

This feature is supported on the following phones:

- Cisco IP Phone 8811
- Cisco IP Phone 8841
- Cisco IP Phone 8845
- Cisco IP Phone 8851
- Cisco IP Phone 8851NR
- Cisco IP Phone 8861
- Cisco IP Phone 8865

Where to Find More Information

- *Cisco IP Phone 8800 Series Administration Guide*
- *Cisco IP Phone 8800 Series User Guide*

User Interface Enhancements

Users can now see the Do Not Disturb(DND) icon displayed in the top line of the phone screen when DND is enabled. Users may also notice a larger displayed font size and an improved line label display.

The administrator does not need to enable these improvements.

These features are supported on the following phones:

- Cisco IP Phone 8811
- Cisco IP Phone 8841
- Cisco IP Phone 8845
- Cisco IP Phone 8851
- Cisco IP Phone 8851NR
- Cisco IP Phone 8861
- Cisco IP Phone 8865

Where to Find More Information

- *Cisco IP Phone 8800 Series Administration Guide*
- *Cisco IP Phone 8800 Series User Guide*

Features Available with the Latest Cisco Unified Communications Manager Device Pack

The following sections describe features in the release which require the new firmware and the latest Cisco Unified Communications Manager Device Pack.

For information about the Cisco Unified IP Phones and the required Cisco Unified Communications Manager device packs, see the following URL:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/devpack_comp_mtx.html

X.509 Digital Certificates Support for EAP-TLS, SCEP, PEAP-GTC

The Cisco IP Phone 8800 Series supports X.509 digital certificates for WLAN authentication. Administrators can use the certificate with WLAN authentication methods:

- Extensible Authentication Protocol-Transport Level Security(EAP-TLS) and Simplified Certified Enrollment Protocol (SCEP)
- Protected Extensible Authentication Protocol (PEAP)-GTC

The Cisco IP Phone 8800 Series can use internal Manufacturing Installed Certificate (MIC) or a User Installed Certificate for EAP-TLS authentication.

This feature is supported on the following phones:

- Cisco IP Phone 8861
- Cisco IP Phone 8865

Where to Find More Information

- *Cisco IP Phone 8800 Series Administration Guide*
- *Cisco IP Phone 8800 Series User Guide*

Installation

Installation Requirements

Before you install the firmware release, you must ensure that your Cisco Unified Communications Manager is running the latest device pack. After you install a device pack on the Cisco Unified Communications Manager servers in the cluster, you need to reboot all the servers.

Note If your Cisco Unified Communications Manager does not have the required device pack to support this firmware release, the firmware may not work correctly.

For information on the Cisco Unified Communications Manager Device Packs, see http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/devpack_comp_mtx.html.

Install the Firmware Release on Cisco Unified Communications Manager

Before using the phone firmware release on the Cisco Unified Communications Manager, you must install the latest Cisco Unified Communications Manager firmware on all Cisco Unified Communications Manager servers in the cluster.

Step 1 Go to the following URL:
https://software.cisco.com/download/navigator.html?mdfid=284729655&flowid=75283

Step 2 Choose **Cisco IP Phone 8800 Series**.

Step 3 Choose your phone type.

Step 4 Choose **Session Initiation Protocol (SIP) Software**.

Step 5 In the Latest Releases folder, choose **11.0(1)**.

Step 6 Select the firmware file, click the **Download** or **Add to cart** button, and follow the prompts:

- For Cisco IP Phone 8811, 8841, 8851, 8851NR, and 8861—cmterm-88xx-sip.11-0-1-10.k3.cop.sgn
- For Cisco IP Phone 8845 and 8865—cmterm-8845_65-sip.11-0-1-10.k3.cop.sgn

Note If you added the firmware file to the cart, click the **Download Cart** link when you are ready to download the file.

Step 7 Click the + next to the firmware file name in the Download Cart section to access additional information about this file. The hyperlink for the readme file is in the Additional Information section, which contains installation instructions for the corresponding firmware.

Step 8 Follow the instructions in the readme file to install the firmware.

Install the Firmware Zip Files

If a Cisco Unified Communications Manager is not available to load the installer program, the following .zip files are available to load the firmware.

- For Cisco IP Phone 8811, 8841, 8851, 8851NR, and 8861— cmterm-88xx.11-0-1-10.zip
- For Cisco IP Phone 8845 and 8865— cmterm-8845_65.11-0-1-10.zip

Firmware upgrades over the WLAN interface may take longer than upgrades using a wired connection. Upgrade times over the WLAN interface may take more than an hour, depending on the quality and bandwidth of the wireless connection.

Step 1 Go to the following URL:
https://software.cisco.com/download/navigator.html?mdfid=284729655&flowid=75283

Step 2 Choose **Cisco IP Phones 8800 Series**.

Step 3 Choose your phone model.

Step 4 Choose **Session Initiation Protocol (SIP) Software**.

Step 5 In the Latest Releases folder, choose **11.0(1)**.

Step 6 Download the relevant zip files.

Step 7 Unzip the files.

Step 8 Manually copy the unzipped files to the directory on the TFTP server. See *Cisco Unified Communications Operating System Administration Guide* for information about how to manually copy the firmware files to the server.

Limitations and Restrictions

Phone Behavior During Times of Network Congestion

Anything that degrades network performance can affect Cisco IP Phone voice and video quality, 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

Health-Care Environment Use

This product is not a medical device and uses an unlicensed frequency band that is susceptible to interference from other devices or equipment.

On-Hook Transfer Limitation in SIP Phones

When the Cisco Unified Communications Manager **Transfer On-Hook Enabled** field is enabled, users might report a problem with direct call transfer in SIP phones. If the user transfers the call and immediately goes on hook before they hear the ring signal, the call may drop instead of being transferred.

The user needs to hear the ring signal so that they can be sure that the call is being routed.

View Caveats

You can search for caveats using the Cisco Bug Search.

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

Before You Begin

To view caveats, you need the following items:

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

Step 1 Perform one of the following actions:

- Use this URL for all caveats: https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286286015&rls=11.0(1)&sb=anfr&svr=3nH&srtBy=byRel&bt=custV
- Use this URL for all open caveats: https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286286015&rls=11.0(1)&sb=afr&sts=open&svr=3nH&srtBy=byRel&bt=empCustV
- Use this URL for all resolved caveats: https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286286015&rls=11.0(1)&sb=afr&sts=fd&svr=3nH&srtBy=byRel&bt=custV

Step 2 When prompted, log in with your Cisco.com user ID and password.

Step 3 (Optional) Enter the bug ID number in the Search for field, then press **Enter**.

Cisco Unified Communication Manager Public Keys

To improve software integrity protection, new public keys are used to sign cop files for Cisco Unified Communications Manager Release 10.0.1 and later. These cop files have “k3” in their name. To install a k3 cop file on a pre-10.0.1 Cisco Unified Communications Manager, consult the README for the ciscocm.version3-keys.cop.sgn to determine if this additional cop file must first be installed on your specific Cisco Unified Communications Manager version. If these keys are not present and are required, you will see the error “The selected file is not valid” when you try to install the software package.

Unified Communications Manager Endpoints Locale Installer

By default, Cisco IP Phones are set up for the English (United States) locale. To use the Cisco IP Phones in other locales, you must install the locale-specific version of the Unified Communications Manager Endpoints Locale Installer on every Cisco Unified Communications Manager server in the cluster. The Locale Installer installs the latest translated text for the phone user interface and country-specific phone tones on your system so that they are available for the Cisco IP Phones.

To access the Locale Installer required for a release, access http://software.cisco.com/download/navigator.html?mdfid=286037605&flowid=46245, navigate to your phone model, and select the Unified Communications Manager Endpoints Locale Installer link.

For more information, see the documentation for your particular Cisco Unified Communications Manager release.

Note The latest Locale Installer may not be immediately available; continue to check the website for updates.

Cisco IP Phone Documentation Updates on Cisco Unified Communications Manager

The Cisco Unified Communications Manager Self Care Portal (Release 10.0 and later) and User Options web pages (Release 9.1 and earlier) provide links to the IP Phone user guides in PDF format. These user guides are stored on the Cisco Unified Communications Manager and are up to date when the Cisco Unified Communications Manager release is first made available to customers.

After a Cisco Unified Communications Manager release, subsequent updates to the user guides appear only on the Cisco website. The phone firmware release notes contain the applicable documentation URLs. In the web pages, updated documents display “Updated” beside the document link.

Note The Cisco Unified Communications Manager Device Packages and the Unified Communications Manager Endpoints Locale Installer do not update the English user guides on the Cisco Unified Communications Manager.

Administrators and users should check the Cisco website for updated user guides and download the PDF files. Administrators can also make the files available to the users on their company website.

Tip Administrators may want to bookmark the web pages for the phone models that are deployed in their company and send these URLs to their users.

Cisco IP Phone Firmware Support Policy

For information on the support policy for Cisco IP Phones, see http://www.cisco.com/c/en/us/support/docs/collaboration-endpoints/unified-ip-phone-7900-series/116684-technote-ipphone-00.html.

Documentation, Service Requests, and Additional Information

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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.

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: http://www.cisco.com/go/trademarks. 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. (1110R)