Cisco IP Phone 7800 Series Multiplatform Phones Release Notes for Firmware Release 11.3(3)

First Published: 2021-02-01

Release Notes

Use these release notes with the Cisco IP Phone 7800 Series Multiplatform Phones running SIP Firmware Release 11.3(3).

The following table describes the individual phone requirements.

Phone	Support Requirements
Cisco IP Phone 7800 Series Multiplatform Phones	BroadSoft BroadWorks 24.0 MetaSphere CFS version 9.5 Asterisk 11.0

Related Documentation

Use the following sections to obtain related information.

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

New and Changed Features

Contacts Management of the BroadSoft Personal Directory on the Phone

You can set the BroadSoft Personal directory as the target directory to store the newly added contacts. When this feature is enabled, your users can select the new option **Add contact** to add contacts to the target directory on the phone.

To enable this feature, use the field **Add Contacts to Directory Personal** under the section **XSI Phone Service** from **Voice** > **Phone**.

The phone now supports the users to add, edit, and delete the contacts in the BroadSoft Personal directory. It also supports the users to add contacts from recent calls or any types of directories (if enabled), including:

- All directories

- Personal address book
- BroadSoft directory, including the following subdirectories:
  - Enterprise
  - Group
  - Personal
  - Enterprise Common
  - Group Common
- LDAP directory

Where to Find More Information

- *Cisco IP Phone 7800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 7800 Series Multiplatform Phones User Guide*

DNS SRV Support for XMPP

You can use Domain Name System Service (DNS SRV) records to establish connection between the BroadSoft XMPP server and the phone. The phone looks for the IP address of the XMPP server, it first sends DNS SRV query on the given domain name. If there is no A record in the DNS SRV response, then it tires A record lookup for the same domain.

To enable this feature, you can use the **Port** field under the **Broadsoft XMPP** section from **Voice** > **Phone**. The port number must be set to **0**.

Where to Find More Information

- *Cisco IP Phone 7800 Series Multiplatform Phones Administration Guide*

Enable Preconditions

You can enable or disable precondition signaling separately.

As in the previous release, precondition is combined with the 100REL SIP extension. When you enable the 100REL SIP feature, the precondition signaling is enabled at the same time.

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

To enable this feature, you can use the **Precondition Support** field under the **SIP Settings** section from **Voice** > **Ext (n)**.

Where to Find More Information

- *Cisco IP Phone 7800 Series Multiplatform Phones Administration Guide*

HTTP Header Specification for PRT

You can specify the HTTP header for the URL that is used for the PRT upload script.

Only the PRT log collector uses the feature.

To enable this feature, you can use the **PRT HTTP Header** and **PRT HTTP Header Value** fields under the **Problem Report Tool** section from **Voice** > **Provisioning**.

Where to Find More Information

- *Cisco IP Phone 7800 Series Multiplatform Phones Administration Guide*

Show Product Configuration Version

You can customize the product configuration version that shows as the menu item **Configuration version** on the phone screen **Product information**.

To enable this feature, set the value for the element `<Device_Config_Version>` in the phone configuration file (cfg.xml).

Note This is the only method to configure the element.

Where to Find More Information

- *Cisco IP Phone 7800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 7800 Series Multiplatform Phones User Guide*

Softkeys Configuration to Calls History List

You can configure the **Option**, **Call**, **Edit call**, **Filter**, and **Back** softkeys on the screen for All, Placed, Received, and Missed calls list. When you press the **Recents** softkey on the phone, you can directly access the **All calls** screen and see the list of all types of recents calls.

To implement this feature, a new parameter **Broadsoft Call History Key List** is added. In the phone web interface, access this new parameter in the **Programmable Softkeys** section from **Voice** > **Phone** tab. The **Broadsoft Call History Key List** parameter defines the values for the softkeys **Option**, **Call**, **Edit call**, **Filter**, and **Back** for All, Placed, Received, and Missed calls list.

Where to Find More Information

- *Cisco IP Phone 7800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 7800 Series Multiplatform Phones User Guide*

Synchronization of Call Waiting and Anonymous Call Rejection

You can enable synchronization of the Call Waiting and Anonymous Call Rejection functions between a specific line and a BroadSoft server. When enabled, the line gets the latest status of the functions from the BroadSoft server, and the line can put the setting of the functions to the BroadSoft server. For example, if the

functions are disabled on the BroadSoft server, the functions don't work on the line. If the user enables or disables the functions on the line, the setting modifies the status of the functions on the BroadSoft server.

The setting of the synchronization is only available for specific lines. The priority of the synchronized functions is higher than the local call waiting (**CW Setting**) and anonymous call blocking (**Block ANC Setting**) functions. The settings of the local functions are under the **Supplementary Services** section from **Voice** > **User** of the phone administration web page.

To enable synchronization of Call Waiting between a line and an XSI service, use the **Call Waiting Enable** field under the **XSI Line Service** section from **Voice** > **Ext (n)** of the phone administration web page.

To enable synchronization of Anonymous Call Rejection between a line and an XSI service, use the **Block Anonymous Call Enable** field under the **XSI Line Service** section from **Voice** > **Ext (n)** of the phone administration web page.

Where to Find More Information

- *Cisco IP Phone 7800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 7800 Series Multiplatform Phones User Guide*

Unavailable Text Box of Agent Status Control

This feature enables you to control the availability of the **Unavailable** menu text box of the agent status on the phone. To control the display of this text box for each line, use the **Unavailable Reason Code Enable** parameter on the **Voice** > **Ext(n)** tab of the phone administration web page. Set the parameter to **No** to hide the **Unavailable** menu text box.

Where to Find More Information

- *Cisco IP Phone 7800 Series Multiplatform Phones Administration Guide*
- *Cisco IP Phone 7800 Series Multiplatform Phones User 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/286318380

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 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 **11.3.3** 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 corresponding file.

`cmterm-78xx.11-3-3MPP0001-377_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. **a.** On the phone administration web page, go to **Admin Login** > **Advanced**, **Voice** > **Provisioning** > **Firmware Upgrade**.
  2. **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
     ```

     Examples:

     ```
     http://10.73.10.223/firmware/sip78xx.11-3-3MPP0001-377.loads
     ```

     ```
     https://server.domain.com/firmware/sip78xx.11-3-3MPP0001-377.loads
     ```
  3. **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
  ```

  Examples:

  ```
  https://10.74.10.225/admin/upgrade?http://10.73.10.223/firmware/sip78xx.11-3-3MPP0001-377.loads
  ```

  ```
  https://10.74.10.225/admin/upgrade?https://server.domain.com/firmware/sip78xx.11-3-3MPP0001-377.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=286311381&rls=11.3(3)&sb=anfr&bt=custV
- To view open caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311381&rls=11.3(3)&sb=afr&bt=custV
- To view resolved caveats that affect this release:

  https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311381&rls=11.3(3)&sb=fr&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 Phone 7800 Series Multiplatform Phones that use Firmware Release 11.3(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 6.

- CSCvv20301 POR: Not all characters are shown in the character preview pop-up
- CSCvv21588 6821/7811/7832: PSK labels for Extend PSK functionality feature are truncated
- CSCvv51309 MPP software is not completing the ICE procedures when placing a call to L2SIP
- CSCvw21396 ICE, Offer not having ICE candidates should be handled
- CSCvw56643 Will not get the new IP address after changing the VLAN of the switch port
- CSCvw72979 Phone will show the call center softkey after answer executive or call forward call
- CSCvw82717 MPP phones - SBC is rejecting a specific line-seize SIP SUBSCRIBE
- CSCvw87814 Dropped Media from ICE enabled Device on Non ICE Call Path
- CSCvx05499 Two "Anonymous" were shown on LCD when shareline receiving anonymous calls
- CSCvx08073 BS DIR - can't search name containing the non ASCII char like ä
- CSCvx13295 xmpp ping error will not trigger failover

Resolved Caveats

The following list contains the severity 1, 2, and 3 defects that are resolved for the Cisco IP Phone 7800 Series Multiplatform Phones that use Firmware Release 11.3(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 6.

- CSCvi40035 Multiple Vulnerabilities in glibc
- CSCvr76623 CP-7841-3PCC-K9= Conference URI not working
- CSCvs02868 1-way audio on OPUS codec if remote does not send OPUS codec fmt
- CSCvs31787 Linux Kernel drivers/net/wireless/ath/ath9k/htc_hst.c Memory Leak Denial of Service Vulnerability
- CSCvs31891 Linux Kernel adis_update_scan_mode() Function Memory Leak Denial of Service Vulnerability
- CSCvs35093 Linux Kernel i2400m_op_rfkill_sw_toggle() Function Memory Leak Denial of Service Vulnerability
- CSCvs35120 Linux Kernel ath9k_wmi_cmd() Function Memory Leak Denial of Service Vulnerability
- CSCvs44665 Linux Kernel vcs_write Write Access Prevention Vulnerability
- CSCvt06289 Linux Kernel vc_do_resize Function Use-After-Free Vulnerability

- CSCvt18740 Loud buzzing noise when pressing speaker/Class-D Amplifier Damage Issue
- CSCvt22582 libxml2 xmlParseBalancedChunkMemoryRecover Memory Leak Vulnerability
- CSCvt22995 MPP does not show BLF when NOTIFY has different URI
- CSCvt26125 Evaluation of 7800 for expired certificates
- CSCvu51113 GNU dnsmasq DNS Reply Heap Buffer Overflow Vulnerability
- CSCvu62280 Multiple Vulnerabilities in glibc
- CSCvu62299 GNU glibc realpath Function Long Pathname Arguments Arbitrary Code Execution Vulnerability
- CSCvu68891 Parser error when tag on header in INVITE contains more than 79 characters
- CSCvu70127 Multiple Vulnerabilities in glibc
- CSCvw30731 MPP phones - "DHCP Option To Use" value revert back to default

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)