Cisco Unified IP Phone 8961, 9951, and 9971 (SIP) Release Notes for Firmware Release 9.0(3)

Revised: August 03, 2010

Use these release notes with a Cisco Unified IP Phone running SIP firmware release 9.0(3). This version of firmware release 9.0(3) is compatible with Cisco Unified Communications Manager (Unified CM) 7.1(3) and later.

Contents

These release notes provide the following information. You might need to notify your users about some of the information provided in this document.

Related Documentation

Cisco Unified IP Phone 9951 and 9971 Documentation

Refer to publications that are specific to your language, phone model and Cisco Unified Communications Manager release. Navigate from the following documentation URL:

http://www.cisco.com/en/US/products/ps10453/tsd_products_support_series_home.html

Cisco Unified IP Phone 8961 Documentation

Refer to publications that are specific to your language, phone model and Cisco Unified Communications Manager release. Navigate from the following documentation URL:

http://www.cisco.com/en/US/products/ps10451/tsd_products_support_maintain_and_operate.html

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco Unified Communications Manager Documentation

Refer to the Cisco Unified Communications Manager Documentation Guide and other publications specific to your Cisco Unified Communications Manager release. Navigate from the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Cisco Unified Communications Manager Business Edition Documentation

Refer to the Cisco Unified Communications Manager Business Edition Documentation Guide and other publications that are specific to your Cisco Unified Communications Manager release. Navigate from the following URL:

http://www.cisco.com/en/US/products/ps7273/tsd_products_support_series_home.html

New and Changed Information

This section contains these sections:

Call-Forward-All Upgrade for CTI New Call Event

With firmware release 9.0(3), information was added to the Computer Telephony Integration (CTI) new call event. The JTAPI and TAPI applications can now distinguish between an actual outgoing call and a call that is created when a user presses the call-forwarding softkey (CFwdALL or Forward All depending on the IP phone model), or presses the Forward All line button on the Cisco Unified IP Phone 8961, 9951, and 9971.

This enhancement applies only if the Call Forward All feature is invoked when the phone is on hook. If the phone is off hook, such as when a user lifts the handset or presses the speakerphone before invoking the Call Forward All feature, the CTI new call event will not provide the call-forward-all information.

In-service Upgrade Enhancement

The dual-banked firmware update feature allows the Cisco Unified CM administrator to upgrade phone firmware with a new load before resetting the new load to an Inactive load status. Instead of waiting for all the phones to download the firmware, Cisco Unified CM administrators can use the Switch Loads function to quickly switch from the old load to the new load in less time. Upgrading the dual-banked firmware reduces the bandwidth congestion and the delay in download during system maintenance while allowing Cisco Unified CM administrators to determine when to set the new firmware to Active load.

Note During dual-banked firmware upgrade, the previous Active load is swapped as an Inactive load. No change is made if the new load matches with the Active load settings. If there is no previous Active load, (fresh install), the Inactive load setting is empty.

A new area in Cisco Unified CM Administration Device Settings Configuration allows you to change the Active load and the Inactive load. Go to **Cisco Unified CM Administration > Device > Device Settings > Device Defaults > Dual Bank Information** area to change the load.

The In-service Upgrade Enhancement feature is supported on these IP phones running the SIP protocol:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Secure and Nonsecure Indication Tone

With firmware release 9.0(3), the secure indication tone functionality was updated, and the nonsecure indication tone was added to the Secure and Nonsecure Indication Tone feature for the Cisco Unified IP Phones. The 8.0(3) release of Cisco Unified Communications Manager (Unified CM) is a requirement for these changes to function.

If phone is configured as secure (encrypted and trusted) in Unified CM, it can be given a "protected" status (which is separate from the status a call). After that if desired, the protected phone can be configured to play an indication tone at the beginning of a call:

- Protected Device—To change the status of a secure phone to protected, check the "Protected Device" check box in Cisco Unified Communications Manager Administration > Device > Phone > Phone Configuration.
- Play Secure Indication Tone—To enable the protected phone to play a secure or nonsecure indication tone, set the "Play Secure Indication Tone" to True. (The default is False.) You set this option in Cisco Unified Communications Manager Administration > System > Service Parameters. Select the server and then the Unified CM service. In the Service Parameter Configuration window, select the option in the Feature - Secure Tone area. (The default is False.)

Only protected phones hear secure or nonsecure indication tones. (Nonprotected phones never hear tones.) Because the condition for playing the secure indication tone is now based on the overall secure status of the call end to end and not the protected status of the phone, users hear a tone between a protected phone and a nonprotected phone if the Secure Real-Time Transfer Protocol (SRTP) or Real-Time Protocol (RTP) is established.

If the overall call status changes during the call, the indication tone changes accordingly. At that time, the protected phone plays the appropriate tone.

A protected phone plays a tone or not under these circumstances:

- When the option to play a tone, "Play Secure Indication Tone," is enabled (True):
  - When end-to-end secure media is established through the Secure Real-Time Transfer Protocol (SRTP) and the call status is secure, the phone plays the secure indication tone (three long beeps with brief pauses).
  - When end-to-end nonsecure media is established through the Real-Time Protocol (RTP) and the call status is nonsecure, the phone plays the nonsecure indication tone (six short beeps with brief pauses). (This capability is a change with this release.)

- When the Play Secure Indication Tone option is disabled (False), no tone is played.

These changes were also made with this release:

  - Users can invoke supplementary services, such as Transfer or Conference, from protected phones without a software limitation.
  - In the past if calls were transferred from a protected phone to another protected phone with RTP established, the call would be dropped. Now users hear a secure or nonsecure indication tone instead of the call being dropped.

The Secure and Nonsecure Indication Tone feature is supported on these IP phones running the SCCP and SIP protocol:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Non-CDP Power Negotiation

For firmware release 9.0(3), the Non-CDP Power Negotiation feature allows the phone to use up to 15.4 watts (the AF maximum) without negotiation. You can disable CDP on the phone configuration window in Cisco Unified CM administration.

The Non-CDP Power Negotiation feature is supported on these IP phones running the SIP protocol:

- Cisco Unified IP Phone 9971
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 8961

Secure Extension Mobility

Communication exchanged between a Cisco Unified IP Phone service and other applications uses the HTTPS protocol, which ensures that all information is secure. When users log into Cisco Unified CM applications, they provide authentication information. User credentials are encrypted after the change of the communication protocol to HTTPS. Web applications with both HTTP and HTTPS support have two URLs configured. Cisco Unified IP phones that support HTTPS select the HTTPS URL; otherwise, the phone select the HTTP URL.

The Extension Mobility HTTPS Support feature is supported on these IP phones running the SIP protocol:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Secure SIP Failover for SRST

Firmware release 9.0(3) provides support for secure calls on a Cisco Unified IP Phone running the SIP protocol to remain secure once the call fails over to SRST from Cisco Unified Communications Manager. In addition, this feature enables the user to verify that the call is still secure by the lock icon that remains on the phone display.

For firmware release 9.0(3), when an IP phone endpoint using SIP is in a secure call that fails over to SRST from Unified CM, the user will continue to see the lock icon on the phone display, indicating the call remains secure. In previous releases, an SIP/TLS/TCP call that fails over to SRST displayed the play arrow icon to indicate a non-secure call.

The SRST supports RTP and SRTP media connections according to how the security settings are configured on the IP Phone.

The system administrator configures SRST on a Cisco router to allow endpoints using SIP to register to SRST using SIP/UDP, SIP/TCP, and SIP/TLS/TCP.

An example of a complete secure configuration for the SRST is shown below:

```
voice service voip
srtp fallback
allow-connections sip to h323
allow-connections sip to sip
sip
    url sips
    srtp negotiate cisco
voice register global
security-policy secure
sip-ua
registrar ipv4:101.2.0.10 expires 3600
xfer target dial-peer
crypto signaling default trustpoint 3745-SRST strict-cipher
```

The default value for the CLI command security-policy is **device-default**. If the value is set to the default value, the existing transport mechanism will be accepted by and registered to the SRST on failover. If the value is set to **secure**, the SRST will only accept the following transport mechanisms in order to ensure the call maintains its secure state, if applicable—SIP/TLS/TCP.

An example of a complete device-default configuration for the SRST is shown below:

```
voice service voip
srtp fallback
allow-connections sip to h323
allow-connections sip to sip
sip
    url sip
    srtp negotiate cisco
voice register global
default security-policy
sip-ua
registrar ipv4:101.2.0.10 expires 3600
xfer target dial-peer
crypto signaling default trustpoint 3745-SRST
```

In firmware release 9.0(3), when an IP Phone endpoint using SIP is in a secure call that fails over to SRST from Unified CM, the user will continue to see the lock icon on the phone display, indicating the call remains secure. In previous releases, an SIP/TLS/TCP call that fails over to SRST displayed the play arrow icon to indicate a non-secure call.

The Secure SIP Failover for SRST feature is supported on these IP phones running the SIP protocol:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Trust Verification Service and Security

To support secure connections with other components, a Cisco Unified IP Phone authenticates component certificates by validating the certificates with entries in the Certificate Trust List (CTL) file, which has a 32-character maximum limit.

The Trust Verification Service (TVS) allows the phone to authenticate components without adding a CTL file entry. Adding new components or services does not require the CTL file to be updated on all of the phones.

The Security by Default feature removes the restriction that requires the user to create the CTL file by using eTokens to provide and enable security features. The signed file is enabled automatically by default.

The Trust Verification Service and Security by Default feature is supported on these IP phones running the SIP protocol:

- Cisco Unified IP Phone 8961
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 9971

Installation Notes

This section contains these sections:

Installing Cisco Unified Communications Manager

Before using the Cisco Unified IP Phone with Cisco Unified Communications Manager, you must install the latest firmware on all Cisco Unified Communications Manager servers in the cluster.

Note You can install Cisco Unified Communications Manager 7.1(3) or 7.1(3a). After you install one of these releases, you must install Cisco Unified Communications Manager 7.1(3a)su1.

To download and install the Cisco Unified Communications Manager version, refer to the Install and Upgrade Guides for Cisco Unified Communications Manager.

Installing Firmware Release 9.0(3) for SIP

To download and install the phone firmware, follow these steps:

Procedure

Step 1 Go to the following URL:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240

Step 2 Log in to the Tools and Resources Download Software page.

Step 3 Click **+** and choose the **IP Telephony** folder.

Step 4 Click **+** and choose the **IP Phones** folder.

Step 5 Choose **Cisco Unified IP Phones 9900 Series** or **Cisco Unified IP Phones 8900 Series**.

Step 6 Choose your phone type.

Step 7 Under the **Latest Releases** folder, choose **9.0(3)**.

Step 8 Select one of the following firmware files, click the **Download Now** or **Add to cart** button and follow the prompts.

- **cmterm-8961.9-0-3.cop.sgn**
- **cmterm-9951.9-0-3.cop.sgn**
- **cmterm-9971.9-0-3.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 9 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:

- **cmterm-8961.9-0-3-readme.html**
- **cmterm-9951.9-0-3-readme.html**
- **cmterm-9971.9-0-3-readme.html**

Step 10 Follow the instructions in the Readme file to install the firmware.

Note 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.

Installing Cisco Unified Video Camera Firmware

To use the Cisco Unified Video Camera on the Cisco Unified IP Phone 9971, you must install the IP phone firmware that supports video for the camera.

Note The Cisco Unified Video Camera is supported on Unified CM versions 7.1(3a)su1 and later.

Procedure

Step 1 Go to the following URL:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240

Step 2 Log in to the Tools and Resources Download Software page.

Step 3 Click **+** and choose the **IP Telephony** folder.

Step 4 Click **+** and choose the **IP Telephony** folder.

Step 5 Click **+** and choose the **Call Control** folder.

Step 6 Click **+** and choose the **Cisco Unified Communications Manager (CallManager)** folder.

Step 7 Choose **Cisco Unified Communications Manager Version 7.1**.

Step 8 Choose **Unified Communications Manager/CallManager Device Packages**.

Step 9 Under the **Latest Releases** folder, choose **7.1(3.33031)**.

Step 10 Select **cmterm-devicepack7.1.3.33031-1.cop.sgn**, click the **Download Now** or **Add to cart** button and follow the prompts.

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

Step 11 Click the **+** next to **cmterm-devicepack7.1.3.33031-1.cop.sgn** 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 device package firmware file.

Step 12 Follow the instructions in the Readme file to install the firmware.

Important Notes

This section contains these topics:

Using a USB Hub During an Active Call

If you use a USB hub on your IP phone or expansion module, do not unplug the hub while you are on an active call. Unplugging the hub in this scenario may cause the IP phone or expansion module to reboot. For more information, refer to CSCtf46146 using the Software Bug Toolkit.

Using a USB Headset

When you use any USB headset that uses an external power source with the Cisco Unified IP Phone, the headset must be used with external power connected only.

Note When using your USB headset with a Cisco Unified IP Phone, do not unplug the headset while you are on an active call. This may cause the IP phone to reboot. For more information, refer to CSCte96060 using the Software Bug Toolkit.

Note To use the Plantronics CS50 headset for incoming calls, press the headset button once to answer a call. Press the headset button twice to go offhook.

Using the USB Headset with the Cisco Unified IP Color Key Expansion Module

The Plantronics CS50 USB headset causes the phone to request power from switch even though it is self-powered. In this case, if a device such as a camera or expansion module is connected and active on the phone, the switch will reject the power request for the headset because the power budget has been exceeded. In this case, the headset cannot be used.

One-Way Video Calls for the Cisco Unified IP Phone

Due to limitations in the H.264 video signaling standards, Cisco Unified IP Phones 9951 and 9971 may not correctly display video received from devices supporting resolutions greater than 640x480. In this case, the user will see a black video window.

To insure that video from such devices is properly displayed on the IP phone, the best solution is to configure high definition phones and Cisco Unified IP Phone 8961, 9951, and 9971 into different call regions and limit the video bandwidth to 384 kb/s when calling between regions.

Tracking the Cisco Unified IP Phone 9971 using Cisco Emergency Responder

You must configure the Cisco Unified IP Phone 9971 in Wi-Fi mode. When using this phone in this mode, you need to configure Cisco Emergency Responder appropriately for tracking wireless IP Phones. For more information, refer to chapter 5 of the *Cisco Emergency Responder Administration Guide 8.0*.

Web Access Disabled by Default

Access to all web services, such as HTTP and SSH, are disabled by default on the Cisco Unified IP Phone 8961, 9951, and 9971. Your administrator can enable this feature by using Enterprise parameters.

Note Enabling web services may cause security problems.

Caveats

This section contains these topics:

Using Bug Toolkit

Known problems (bugs) are graded according to severity level. These release notes contain descriptions of:

- All severity level 1 or 2 bugs.
- Significant severity level 3 bugs.

You can search for problems by using the Cisco Software Bug Toolkit.

To access Bug Toolkit, you need the following items:

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

To use the Software Bug Toolkit, follow these steps:

Procedure

Step 1 To access the Bug Toolkit, go to:

http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs.

Step 2 Log on with your Cisco.com user ID and password.

Step 3 To look for information about a specific problem, enter the bug ID number in the "Search for bug ID" field, then click **Go**.

Open Caveats

Table 1 lists Severity 1, 2 and 3 defects that are open for the Cisco Unified IP Phone using firmware release 9.0(3).

For more information about an individual defect, you can access the online record for the defect by clicking the Identifier or going to the URL shown. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, be aware that Table 1 reflects a snapshot of the defects that were open at the time this report was compiled. For an updated view of open defects, access Bug Toolkit as described in the "Using Bug Toolkit" section on page 10.

Table 1 Open Caveats for Firmware Release 9.0(3)

Identifier	Headline and Bug Toolkit
CSCtf59793	Only the first 63 characters of DHCP option 66 value are used
CSCtf61730	Unable to play ringtone after volume adjustment
CSCtf69028	No DNS query for Unified CM name after the second reset
CSCtf72234	IP phone firmware load returns 0.0.0.0 regardless of the server used
CSCtf82731	Cisco Unified IP Phone 9971 with 802.11a cannot refresh the GUI automatically when WLAN site survey is selected

Table 1 Open Caveats for Firmware Release 9.0(3) (continued)

Identifier	Headline and Bug Toolkit
CSCtf83026	The “Active Calls” softkey turns gray, sometimes, when joining two conferences
CSCtg00123	User of a Cisco Unified IP Phone 9971 with WI-FI cannot hear the peer voice when on an active call for an extended period
CSCtg07000	sRTCP authentication tag must be 80 bits
CSCtg16900	Specific IP address and port value do not exist in TCLAS message
CSCtg17243	Java application fails after user locale transfer from Arabic to Greek
CSCtg21655	Cisco Unified IP Phone displays an error when attempting to capture a screenshot
CSCtg35553	Static WEP key is lost when you power cycle a Cisco Unified IP Phone 9971
CSCtg35553	Static WEP key is lost after power cycling a Cisco Unified IP Phone 9971
CSCtg41425	Video stream information reports incorrect number of RTCP receiver reports sent
CSCtg41863	Cisco Unified IP Phone 9951 goes into call preservation mode
CSCtg44001	Chaperone recording is not resumed when the analyst is brought to conference
CSCtg55784	Impairments in VGA video received from Cisco Unified Communication Integration for Microsoft Office Communicator (CUCIMOC) quality assurance drop nine by IP phone
CSCtg61756	IP phone registers and resets in loop with 128-character end user
CSCtg70515	The call record is highlighted after a selecting it three times
CSCtg75012	The “play” softkey is always grayed out after the IP phone plays a ringtone
CSCtg77953	Removing the IP phone NTP reference does not work
CSCtg81191	New IP phone has no applications when used for the first time
CSCtg88583	The USB camera is not detected after a firmware change
CSCth34088	First connection with the Bluetooth headset icon fails after first pairing

Resolved Caveats

Table 2 lists Severity 1, 2 and 3 defects that are resolved for the Cisco Unified IP Phone using firmware release 9.0(3).

For more information about an individual defect, you can access the online record for the defect by clicking the Identifier or going to the URL shown. You must be a registered Cisco.com user to access this online information.

Because defect status continually changes, be aware that Table 2 reflects a snapshot of the defects that were resolved at the time this report was compiled. For an updated view of resolved defects, access Bug Toolkit as described in the “Using Bug Toolkit” section on page 10.

Table 2 Resolved Caveats for Firmware Release 9.0(3)

Identifier	Headline and Bug Toolkit
CSCta65070	WLAN is choppy
CSCtc85364	Java application downloads but is not installed
CSCtc87897	Dial tone is heard on IP phone during RTP streaming using RTPTx

Table 2 Resolved Caveats for Firmware Release 9.0(3) (continued)

Identifier	Headline and Bug Toolkit
CSCte51956	Failure to access the HTTPS server of the IP phone
CSCte55948	Session background color is not correct when java application is closed during a call
CSCte64869	Perfect Forward Security (PFS) is hung with constant keep alives and never exits
CSCte67016	IP Phone resets while using Bluetooth headset
CSCte68858	Secure IP phone does not show SRST as “standby” after fallback
CSCte72048	IP phone becomes unresponsive after moderate HTTP and HTTPS web access
CSCte72752	IP phone will not restart even when it receives a restart request from Unified CM
CSCte73474	No tone after holding and resuming a monitored call
CSCte77981	IP phone is not able to login to Extension Mobility Cross Cluster (EMCC) when service provisioning is set to “External”
CSCte79069	IP phone undergoes an extra reset after a firmware load upgrade
CSCte80842	IP phone (SIP) does not display status line message
CSCte90297	IP phone shows incorrect (its own) directory number in call bubble during conference scenario
CSCte90567	Call forward notification is not produced when IP phone registers with secure SRST
CSCte91025	IP phone web page access using HTTP and HTTPS (alternate) takes a long time
CSCte95590	IP phone needs to download Certificate Trust List (CTL) or Identity Trust List (ITL) after fallback from SRST
CSCte98353	Atypical state after busy tone
CSCte99279	RFC 2833 packets may cause jitter buffer problems with iLBC and iSAC streams
CSCtf07125	IP phone (SIP) should not get stuck requesting a default configuration file
CSCtf08894	Audio arrives after video, ten minutes into a call
CSCtf25128	Speaker LED does not illuminate on redial using the speakerphone button
CSCtf32361	IP phone makes noise in idle mode after making call from “Edit Dial” screen
CSCtf34113	Using a headset during an active PSTN call has one-way audio
CSCtf38735	Session is disconnected if a remote held call is resumed
CSCtf40690	User cannot exit ringtone configuration page when IP phone is partially registered
CSCtf44427	Intercom call cannot be canceled if speakerphone button is pressed
CSCtf44834	An external service is inoperable sometimes if it is loaded continually
CSCtf46340	IP phone load cancel transfer fails
CSCtf48340	Sometimes the video is blocky for several seconds after a video unmute
CSCtf54554	Key expansion module side USB port is disabled intermittently during bootup
CSCtf54801	PFS sometimes does not exit and cannot be halted
CSCtf55462	IP phone drops the active call if “apply configuration” is done with TFTP down
CSCtf63196	Cisco Unified IP Phone reboots while using Bluetooth headset
CSCtf65807	HTTPS server issues while accessing IP phone web page
CSCtf65949	Headset audio stops if second incoming call is unanswered

Table 2 Resolved Caveats for Firmware Release 9.0(3) (continued)

Identifier	Headline and Bug Toolkit
CSCtf69411	Incorrect behavior in conference with SRST; call drops on incorrect IP phone
CSCtf70173	“CiscoIPPhoneDisplay” header reports physical versus usable size
CSCtf70190	Maximum size .png image appears distorted
CSCtf75286	Sometimes the speakerphone button is not lit when receiving an intercom call
CSCtf77362	Restarting the IP phone causes the Busy Lamp Field (BLF) line on expansion module to lose functionality
CSCtf82189	OpenSSL record of termination issue
CSCtf92299	The recipient can unmute a one-way whisper call
CSCtf94811	Voice synchronization measures video ~200ms ahead of audio when audio RTP is delayed
CSCtg04851	Cisco Unified IP Phone 9971 continues to transmit at 768K even after reinvitation for 384K
CSCtg07539	Modify “vcm_tone_start_with_speaker” call to use “lsm_get_ms_ui_id”
CSCtg09883	In call preservation mode the mute key does not function
CSCtg11357	Repeatedly posting XML to IP phone causes it to reset
CSCtg11848	Camera RTCP “sr” time needs adjustment
CSCtg26554	Only one-way audio can be setup for the basic call when using an iSAC codec

Obtaining Documentation and Submitting a Service Request

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/en/US/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.