Avaya IP Deskphone H.323 Release 6.6.0 Readme

This file is the Readme for the Avaya IP Deskphone H.323 Release 6.6.0 for the 9608, 9608G, 9611G, 9621G, 9641G, 9641GS IP Deskphones. This file describes the contents of the April 2015 (6.6.0.29) software distribution package.

H.323 6.6.0 software is supported on the 9608, 9608G, 9611G, 9621G 9641G and 9641GS IP Deskphones only and when used with Avaya Aura® Communication Manager. The H.323 6.6.0 software will not load or operate on any other models.

This release supersedes all previous Avaya IP Deskphone H.323 6.x.x software releases. Avaya recommends that all customers using Avaya IP Deskphone H.323 6.x.x software upgrade to this version at their earliest convenience.

The information in this document is accurate as of the issue date and subject to change.

Please refer to the advisements in this file for important information prior to deploying this software.

Minimum IP Deskphone Software Releases

The 9611G IP Deskphone Global (Comcode 700504845/700501429) must use either Deskphone H.323 6.4.0.14 or later software Deskphone SIP 6.4.0.33 or later software.

The 9608G IP Deskphone (Comcode 700505424/ 700507946) and 9608 IP Deskphone Global (Comcode 700504844/700507947) must use either Deskphone H.323 6.3.1.16 or later software or Deskphone SIP 6.3.1.13 or later software.

The 9641GS IP Deskphone (Comcode 700505992/700509409/700509981) must use either Deskphone H.323 6.6.0.25 or later software or Deskphone SIP 6.5.0.17 or later software.

Attempts to downgrade these models to lower versions of software will be rejected. If these models are implemented in an environment that uses lower versions of software for other 9601/9608/9611G/9621G/9641G IP Deskphones, it is recommended to use a mechanism to differentiate the software loads such as different HTTP servers or different GROUPs.

Avaya Aura® Communication Manager Compatibility

Although the 9608, 9608G, 9611G, 9621G, 9641GS and 9641GS IP Deskphones are supported on Avaya Aura® Communication Manager 6.2 and later, Avaya recommends you to deploy the deskphones and conference phone with the latest available Communication Manager release. See the "Communication Manager Software & Firmware Compatibility Matrix" at http://support.avaya.com for the supported software/firmware versions of the Media Server, Media Gateway, and circuit packs.

CM 6.2 is the minimum version required for *native* support of the 9608, 9608G, 9611G, 9621G, 9641G, 9641GS IP deskphones.

For more details see the H.323 configuration section in the Communication Manager Administration Guide which you can download at http://support.avaya.com.

New features in H.323 6.6.0

Phone functionality and administrative features for 9608, 9608G, 9611G, 9621G, 9641G, and 9641GS IP Deskphones:

- Support 9641GS which has the same functionality as 9641G with the following differences:
    - The 9641GS screen is 5.0 inch TFT screen and it is capacitive screen compare to 4.7 inch resistive TFT screen on the 9641G. The capacitive screen provides highly touch sensitivity and a brighter and sharper look.
    - 9641GS supports Ethernet link and activity LED for the network port.
    - 9641GS supports H.323 6.6.0 or later software and blocks downgrade to earlier releases of software
    - 9641GS BT stack version is BT3.0+EDR (compare to BT2.1+EDR stack version for 9641G)

The 9641G and 9641GS IP Deskphones are using a new Bluetooth stack. *When upgrading to 6.6.0 from an earlier release of software, all Bluetooth devices are removed from the phone and user will need to pair all devices again.*

- Security hardening as part of UCR2013 and JITC testing
    - Support H.323 signaling over TLS ("H323TLS" in addition to "challenge" and "pin-eke" security profiles). Gateway discovery is done as before over UDP, but registration and signaling is done over TLS to port 1300. Certificate signature validation is done as part of opening TLS connection to CM. This feature is supported in non-TTS mode and with PE only (no CLAN).

      Note: There is an option to disable H.323 signaling over TLS in CRAFT menu for debugging purposes.

      This feature requires administration on CM. For more information, refer to the Administering Avaya Aura Communication Manager Administration guide.
    - Support OCSP (Online Certificate Status Protocol) for checking whether certificates presented to the phone by servers are good, revoked, or unknown. If a certificate is revoked, the TLS connection will not be established or will be closed (in the case of ongoing TLS connection).

      In the case of an unknown status, OCSP_ACCEPT_UNK will be used to determine whether to close the connection.

      OCSP responder URL can be used from the certificate presented by the server or locally configured on the phone (OCSP_URI). OCSP_URI_PREF specifies the preference between the two sources.

      OCSP_TRUSTCERTS shall be used for cases where the OCSP response is not signed by a certificate issued by the same CA that issued the certificate that is being checked.

      OCSP is supported for 802.1x (EAP-TLS), IPSec VPN (when certificates are used for authentication), SSO, H.323 signaling over TLS, File downloads, Backup/Restore, WML browser and SLA monitor.
    - FIPS 140-2 cryptographic libraries– when this feature is enabled, cryptographic operations will be done using FIPS 140-2 certified algorithms. The configuration parameter is FIPS_ENABLED set in the settings file.

      The following features support secure operations when FIPS mode is enabled:

- The crypto random generator complies with [SP 800-90] DRBG specification.
- Certificate signature authentication
- H.323 signaling over TLS
- SRTP (only "1-sertp-aescm128-hmac80" mode is supported)
- Settings and upgrade file, trusted certificates, and PKCS#12 files download over HTTPS
- Backup and restore over HTTPS
- OCSP

- Support periodic tests of certificate expiration or revocation for ongoing TLS connections according to SERVER_CERT_RECHECK_HOURS. This parameter is only used when H.323 signaling is over TLS connections.

- Validation of the server identity, as presented in subjectAltName / common name in the Subject field with the server IP or hostname configuration (for example, MCIPADD, TLSSRVR, etc.). The new configuration parameter is TLSSRVRVERIFYID which obsoletes TLSSRVRID (which was not supported in previous releases).

- Support configurable timer (CERT_WARNING_DAYS) for checking the expiration of trusted certificates, identity certificate, and OCSP certificate. This parameter specifies how many days before the expiration of a certificate that a warning should first appear on the phone screen. The notification on the phone screen will be shown with the details of the certificate about to be expired. In addition, syslog/log shall be sent/generated.

- Support downloads of the PKCS12 file (for cases where SCEP is not used). The setting file parameter PKCS12URL defines the URL of the file. There is an option to add a MAC address or serial number to the filename to allow different PKCS#12 files for each phone.

- Support secure renegotiation as specified in IETF RFC 5746. There is an option to enable/disable secure renegotiation according to TLS_SECURE_RENEG for cases where old servers are used that do not provide this support.

  Note: It is highly recommended to support secure renegotiation on both the phone and the server.

- Support certificate signature validation for certificates with a SHA 256 With RSA Encryption signature.
- Support download of intermediate certificates for cases where servers do not provided the full chain up to the root CA. There is no support for certificate signature validation up to intermediate certificate. Certificate signature validation is always supported up to the root CA.

- New VLAN separation scheme – A new configuration parameter VLANSEPMODE was added (in addition to VLANSEP that shall be set to 1) that enforce full separation between PC port and phone for both tagged and untagged traffic when L2QVLAN<> PHY2VLAN (and both has value different than 0), L2Q is auto (0) or (1) tagging. In this new VLAN separation scheme:

        - Packets from PC port will be forwarded to network port unmodified. Tagged packets from PC port will be forwarded to network port only in case their VLAN is equal to PHY2VLAN.
        - Untagged packets from the network will be sent to the PC port only.
        - Tagged packets from the network port will be sent to the PC port if their VLAN is equal to PHY2VLAN and to the phone if their VLAN is equal to L2QVLAN.
        - 802.1x/LLDP and Spanning tree packets are supported as in previous releases in this new mode.
        - When VLANSEPMODE is 0, untagged packets from PC port can reach the phone.
    - Support 2048 bits asymmetric key length for SSH server.
    - Ability to view the SSH fingerprint under the SSH CRAFT menu.
- Disable SSLv3 as result of "POODLE" vulnerability (CVE-2014-3566). Customers are encouraged to validate their servers support TLS 1.0 and later versions before upgrading to 6.6 release.
- IP office support enhancements:
    - Support SRTP with the IP Office 9.1 platform.
        - Support srtp-aescm128-hmac80 SRTP (RFC 3711) cipher suite only.
        - Support SRTP encryption and authentication and SRTCP authentication only.
    - Annex-H signaling support (in addition to challenge).
    - Support deployment of H.323 phones in IP office cloud.
    - Support of Korean and Japanese (9.1 FP)
    - Support wideband Codec icon and Local Network Quality icon in IP Office environment.
- Support Korean and Russian keyboard layout
- Support Thai language file when working with Avaya Communication Manager. There is a new Thai keyboard support. mlf_Sxyz_vn_thai.txt is Thai language file name that shall be configured in one of the LANGxFILE configuration parameters.
- Enhanced local dialing rules are supported for contacts (in addition to call history, etc.). Value 2 is now supported by ENHDIALSTAT configuration parameter in the 46xxsettings.txt file.
- Support key usage for identity certificate generation using SCEP by setting the relevant bits in the certificate request according to MYCERTKEYUSAGE configuration parameter.
- Support DHCP option 43 for configuration of TLSSRVR, TLSDIR, TLSPORT, HTTPSRVR, HTTPORT, HTTPDIR,MCIPADD, L2Q, PHY1STAT, PHY2STAT, PROCSTAT, SIG, TLSSRVRVERIFYID, L2QVLAN.
- Support 802.1Q tagging with VPN packets according to VPNALLOWTAGS configuration parameter which is already supported by 96x0 H.323 3.1.5.
- Support sending packets to PC port from the network unmodified to preserve 802.1Q tagging if exist based on PHY2TAGS configuration parameter which is already supported by SIP R6.3.
- Support configurable Duration of Unsuccessful Discovery Timer up to 16 hours using UDT configuration parameter. This parameter will control the time according which the

phone perform registration discovery and after which the phone will reboot.

- Support automatic labeling for line and bridge appearances where "a."-"z." lowercase (and then "A."-"Z) are added before the line or bridge appearance label. The feature is intended for cases where multiple bridge appearances are shared across few users and there is a need to have a common identifier for each bridge appearance in a way users can communicate between them which bridge to pick up among multiple bridge appearances with different call states (ringing, active, idle, etc.). The labels remain unchanged independent to the call state. CADISPMODE is the configuration parameter.
    - Note: this feature is not supported when using Button Module.
- Keep the active/hold call highlighted when there is incoming call to preserve the call control softkeys unchanged. The new mode is useful for cases where users prefer to have the highlight of their active call unchanged in case of incoming call and to not present the call control soft keys for incoming call. This mode is controlled by CALLAPPRSELMODE configuration parameter.
- Hide "Drop", "Transfer", "Conference" and "Hold" soft key buttons when the phone is registered to Avaya communication manager as call center agent according to the new configuration parameters: CCBTNSTAT, HOLDSTAT, XFERSTAT, CONFSTAT and DROPSTAT which are already supported by 16xx H.323 R1.3.3.
- Support sending "+" to Avaya communication Manager.
- SLA Monitor Agent security enhancements:
    - Removal of embedded Avaya SIP root CA certificate used by SLA mon agent to authenticate the SLA mon server. There will be no more default certificate for SLA mon agent and TRUSTCERTS shall be configured with relevant trusted certificate when SLA mon agent is used.
    - SLMADDR should be configured to the IP address and optional port of the SLA mon server from which the discovery messages shall be received.
    - slamonRootCA.txt will be no longer part of the software distribution file (*.ZIP).
    - SLA functionality in the deskphones is compatible with SLA server release 2.5 and later.
- Increase the size of SCEPPASSWORD to 50 instead of 31.
- Support 4 layer-2 queues on the internal switch instead of 2 queues. This enables a separated handling of data and voice and avoids the audio path being affected by data channel during intensive networking activity behind the PC port.
- Control display of call associated information in the agent information line using AGTCAINFOLINE configuration parameter.
- CALCSTAT shall keep its configuration when file server is not reachable.
- Support SHA-256 on agent greetings files.

Refer to appendix 3 for a list of new parameters associated with this release of software.

Documentation for H.323 6.6.0

The following documents have been updated to support this release of software.

- 9600 Series IP Deskphones Overview and Specification
- Installing and Maintaining Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323
- Administering Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323
- Using Avaya 9608/9608G/9611G IP Deskphones H.323
- Using Avaya 9621G/9641G/9641GS IP Deskphones H.323
- Using 9600 Series H323 in a Call Center
- Avaya 9608/9608G/9611G IP Deskphones H.323 Quick Reference
- Avaya 9621G/9641G/9641GS IP Deskphones H.323 Quick Reference
- Avaya 9608/9608G/9611G/9621G/9641G IP Deskphones H.323 Call Center Quick Reference

These documents are available on http://support.avaya.com under "9600 Series IP Deskphones" -> "H.323 6.6.x" -> Documents

The following documentation has not been updated and is included below for reference.

- Guide to Icons – Avaya 9608/9608G/9611G/9621G/9641G IP Deskphones
- Application Note: EAP-TLS with 9600 Phones
- VPN Setup Guide for 9600 Series IP Deskphones
- Single Sign On for Local Devices – API Guide
- Avaya Deskphone H.323/SIP for 9600 Series – API Guide

H.323 6.6.0 Package Contents

The H.323 6.6.0 software package contains all the files necessary to upgrade Avaya new or previously installed 9608/9608G/9611G/9621G/9641G/9641GS IP deskphones to the H.323 6.6.0 load.

The following files are included in each package:

- S9608_11HALBR6_6_0_29_V474.tar - The 6.6.0 H.323 phone application tar file for 9608 and 9611G models.
- S9621_41HALBR6_6_0_29_V474.tar - The 6.6.0 H.323 phone application tar file for the 9621G, 9641G and 9641GS models.
- S96x1_UKR_V24r26_V24r26.tar – The 6.6.0 H.323 Kernel and root file system tar file.
- 96x1Hupgrade.txt – This file is downloaded by the 9608/9611G/9621G/9641G/9641GS IP deskphones and instructs the phones on how to upgrade. DO NOT EDIT this file. You MUST USE the 96x1Hupgrade.txt file included in this package to upgrade H.323 software.
- 19 predefined language files for phone display:
    - mlf_96x1_V132_arabic.txt
    - mlf_96x1_V132_chinese.txt
    - mlf_96x1_V132_dutch.txt
    - mlf_96x1_V132_english_large.txt
    - mlf_96x1_V132_french_can.txt
    - mlf_96x1_V132_french_paris.txt
    - mlf_96x1_V132_german.txt
    - mlf_96x1_V132_hebrew.txt
    - mlf_96x1_V132_italian.txt
    - mlf_96x1_V132_japanese.txt
    - mlf_96x1_V132_korean.txt
    - mlf_96x1_V132_polish.txt
    - mlf_96x1_V132_portuguese.txt
    - mlf_96x1_V132_russian.txt
    - mlf_96x1_V132_spanish.txt
    - mlf_96x1_V132_spanish_latin.txt
    - mlf_96x1_V132_template_en.txt
    - mlf_96x1_v132_thai.txt
    - mlf_96x1_V132_turkish.txt
- av_csca_pem_2032.txt (Avaya Call Server Root Certificate)
- av_prca_pem_2033.txt (Avaya Product Root CA certificate)
- 96x1mibDRAFT.txt for reference
- AvayaMenuAdmin.txt template for reference
- release.xml

    The signatures in the signatures subdirectory of the .zip distribution packages are only intended to be used by the file server, and the file server that is on the CM6.0 Utility Server is the only file server that currently supports this.

System specific parameters should be entered into the 46xxsettings.txt file which is available for separate download at http://support.avaya.com

The H.323 6.6.0 package is available in the following versions:

- Versions with encryption enabled
    - 96x1-IPT-H323-R6_6_0_29-040715.zip
    - 96x1-IPT-H323-R6_6_0_29-040715.tar
- Versions with encryption disabled
    - 96x1-IPT-H323-R6_6_0_29U-040715.zip
    - 96x1-IPT-H323-R6_6_0_29U-040715.tar

System specific parameters should be entered into the 46xxsettings.txt file which is available for separate download at http://support.avaya.com. **Changed configuration parameters with this release of software are shown in Appendix 3.**

H.323 6.6.0 Resolved Issues

The following table includes the resolved issues which are relevant when the phone is administered by a Communication Manager, Call Center or IP Office:

ID	Issue Description
12151	Deskphones using version 6.6.0 with release prior to 6.6.0.29 lose the trust cert in the following scenario 1) Trust cert is being loaded for the first time. 2) During the next reboot, after having loaded the trust cert, the phone downloads the upgrade file 3) After loading the upgrade file, the deskphone will lose the trust cert if one of the following conditions occur: a. The upgrade file now doesn't have link to the settings file b. The phone is unable to load the settings file due to network problem or file server problem c. The settings file doesn't have now the trust cert settings If one of the conditions in step 4 happened the phone is now running with the Avaya default certificate. Deskphones upgraded from 6.4.0 GA to 6.6.0 load prior to 6.6.0.29 with the trust certificate loaded prior to the upgrade are not impacted by this issue unless administrator will execute reset or clear values. This issue is resolved with this 6.6.0.29 release.
11919	Incorrect Japanese wording to "Loggedout" in v107 language file (SR: 1-6164153251)
11870	When a PC with MVIPTEL application is connected to the phone, the HTTP authentication window might be unexpectedly displayed after registering to the Communication Manager (SR: 1-6046649490).
11711	When enabling the FIPS mode and registering the Communication Manager by an unnamed registration, the phone does not receive dial tone or ringback tone and no voice path is established. CM versions that needed for the correction to work is: 6.3.11 and 6.3.111.
11057	Changing a personalized classic ring tone through the Communication Manager, does not take effect (SR 1-5406481592).
8996	If the administrator executes "Disable nr-registration" in CM, and no other server in the alternate gate keeper list is available, the phones might sometimes remain in discover mode until the alternate gate keeper will become available and won't return to the main, even if "Enable nr-registration" is executed on it.
11569	Release.xml file in the zip package is not written according to the spec (SR: 1-5511004374)
11437	Phone doesn't show the 4th feature button in the quick touch panel even though the QTP is enabled (SR-1-5839279054)
11354	Call transfer soft key is not available when trying to dial through "busy-ind" button and when PHNSCRALL=1 (SR: 1-5529801361)

ID	Issue Description
11333	Button module HW/SW details are not shown in MIB walk (SR:1-5773356675)
11275	Occasionally the phone stops the periodic registration to the Communication Manager after disconnect (SR 1-5571599978).
11161	Caller ID is displayed three times on topline, status line and call appearance while in half screen mode (SR-1-5512555642)
11153	9611 does not move focus to active call appearance in half screen and call center mode (SR-1-5565484635)
11150	Caller ID on topline is not displayed properly on 9641 when PHNSCRCOLUMNS is enabled (SR-1-5530949615)
11147	Phone does not log the incoming call when call is answered by another destination or answered by voice mail (SR-1-5481058245)
11035	The phone doesn't delete custom button label from backup when the button is changed (SR 1-5310649590)
11021	Mute button doesn't allow entering to CRAFT menu after receiving dial tone, even when using double press (SR 1-4643625043)
11020	Deskphone does not take the correct DHCP offer with option 242 (SR:1-5068193759)
10976	Backlight doesn't go off after the phone receives a forwarded call (SR 1-5201836492)
10975 10928	Poor audio quality during a large file upload, when the PC port is connected to a 1GB PC NIC and the LAN port is connected to a 100MB external switch port (SR: 1-5102672831)
10967	When disabling SLA monitor through setting file (SLMSTAT=0), but keeping SLMCAP and SLMCTRL enabled (SLMCAP=1 and SLMCTRL=2), then the craft menu buttons (Service mode control and Service mode record) would be shown as enabled, although SLA Monitor will actually not be working at all.
10839	When configuring the phone with German language, it displays the menu item "Select desired setting" in English instead of German (SR 1-5040817999)
10828	9611 beeps only once instead of ringing continuously when headset is connected and when the incoming call is directed to a hunting group (SR 1-5016509658)
10803	Call log displayed in an incorrect time and order when the call starts before midnight and ended after midnight (SR-1-4995915332)
10802	RTCP packets are not sent occasionally for shuffled calls and causes to the statistics (including round trip delay) to be sent with a zero value(SR: 1-5055274022)
10800	A programmed soft key (SAC) which is displayable on Deskphone, is not displayed on SBM24 (SR 1-4987921834)
10712	In case the settings file already includes the trust certificates list in the TRUSTCERT setting file parameter, then the SLA monitor root certificate must also be added to the list and placed as the first certificate. For example: SET TRUSTCERTS slamonRootCA.crt,rootCertRNAAD.cer
10703	Agent greeting is not played when phone displays vu-stats (SR 1-4662828582)
10620	phone is stuck in discovery mode forever upon registration to wrong extension (SR: 1-4647354675)
10500	Agent greeting is played twice

ID	Issue Description
10494	Entering CRAFT menu require 2 presses on the mute button instead of once after releasing a call in a Call Center environment (SR 1-4643625043)
10473	Fonts are truncated at the bottom of a Button Module 24 when connected to 9608 (SR 1-4708646412)
9542	If the phone is in off-hook idle mode in the following CM versions: CM 6.3 • CM 6.2 SP0 and later • CM 6.0.1 SP 10 and later • CM 5.2.1 SP 14 and later Users may hear a short dial tone sound in the currently active audio device when a failover occurs.
10405	Contact Pairing does not work for unseen calls (SR:1-4622032891)
10370	Screen Saver does not work after an upgrade (SR:1-4639842634)
10346	An unencrypted password is printed for a few milliseconds on login screen (SR 1-4555089071)
10344	When the phone is working in VPN mode, and "NVVPNENCAPS" is configured as if NAT device is used, the phone may become unresponsive.
10279	Very long tone is played during agent login on 9608 (SR 1-4469805575)
10261	Missed call entry is not deleted from All calls and Missed History for extensions with long number and hyphenation format (SR 1-4589576261)
10252	Options & Settings menu option is not displayed when CALLCTRSTAT is 1 and OPSTAT value is set to default (SR 1-4557089616)

H.323 6.6.0 unresolved issues

The following table includes unresolved issues with this release of software which were known as of the issue date for this document.

ID	Issue Description
12135	In some rare cases SNMP will not be available after phone restart. **Solution:** reset again the phone
12001	When feature, call appearance or bridged appearance is added on Station form for an existing station and CADISPMODE is set to 1 the labels set in the wrong order. **Solution:** Disconnect the Button Modules, logout, login and connect the Button Modules.
11469	Call Appearance line numbers does not displays after rebooting the phone when personalize label given for extension.
11886	Phone displays incoming call icon with conference call when CALLAPPRSELMODE and CADISPMODE set to 1.
11981	When deskphone boot up and automatically log in with extension and agent, phone does not always retrieve extension backup file. **Solution:** manually logout and login the extension.
11986	SLA is not supported over VPN.
12026	Entered Thai characters do not display if language changed to English.
11877	When the phone is connected in IP Office environment, the call features (such as call pickup) cannot be accessed from “HOME” screen more than once. **Solution**: go to any other screen, then go back to "HOME" screen and activate the desired call feature again.
11911	Korean only: Entering long personalized labels in feature screen will over write the feature checkbox. **Solution:** Shorten the personalized labels to fit the free space near the checkbox
11806	The value of the settings file parameter “DEFAULTRING” is overridden by the value from the Communication Manager.
11041	Network delay values are high when a call is created between deskphone and E129 endpoints.
10773	When a reset command is sent to the phone using a SAT terminal, talk path is lost but the phone doesn’t reset immediately as expected. **Solution:** The reset will take place after the user disconnects the call.
10907	When the SLMCAP parameter of the settings file is set to 1, the SLA client will not be able to capture packets. **Solution:** Set the value of SLMCAP to 2 to allow capturing of packets.
10873	Agent greeting of type VDN, will not work if VDN name configured on CM exceeds 15 characters. The phone supports 15 characters or less. **Solution:** Configure VDN names on CM to have 15 characters or less.
10861	Incoming calls display the caller name from the CM server, not the local contact name. When the information from the CM server contains an alphanumeric name. For example, if the caller information in the CM is "John 123" and the name is saved in the local contact list as "John W", the phone screen displays "John 123" during the call, and "John W" in the call history.

ID	Issue Description
10859	Changes to the "Match Criteria" field while editing an agent greeting of type VDN/ANI is not saved. **Solution:** Editing any other field in addition to the match criteria will cause the values to be saved - for example change the greeting name by one letter.
10409	The deskphone software supports both the Avaya Communication Manager and the Avaya IP Office Call Managers. A restore to factory defaults is required before switching between the Communication Manager environment and the Avaya IP Office environment. Failing to do so may result in various operational issues. **Solution:** For any abnormal behavior of the phone after switching between CM and IPO, go to CRAFT menu and clear values.
10225	When changing MD5 to TLS and also changing user name on the server, the phone's authentication fails. **Solution:** Clear values through CRAFT menu.
9939	The deskphone supports SRTP AES 128 HMAC 80 cryptographic Suite only. Other cryptographic suites (un-authenticated suites and HMAC 32 based suites) are not supported.
9194	When Cisco Access Control Server (ACS 5.2) is configured for re-authentication timeout, using TLS session tickets to renew authentication, the phone does not re-authenticate. **Solution**: reboot the phone
10118	By opening a second call appearance and start dialing, agents are able to go back to the first call appearance and disconnect the live call.
10642	When configuring the phone for large fonts and the display includes a call forward icon, a ringer off icon and more than 10 missed calls, the Media Quality Indicator would override the time field on the screen. **Solution**: use normal font size when configuring the phone to display a Media Quality Indicator.
10082	Manual restore does not work when there is a logged in contact center agent. **Solution:** Log out the contact center agent, and keep the phone logged in to CM. The manual restore will work correctly at this state. Once the operation completes, log in the contact center agent again.
3609	If CM reboots while an agent is logged in and in Aux-work mode, the headset will remain in off hook mode although the headset led turns off. **Solution**: Make the first incoming or outgoing call and the LED will then start functioning.
7864	In some cases, when you move a phone between two CM servers that have the same station number with different configurations, the phone will not load the new configuration. **Solution**: Open the station details screen in CM and perform any update to the form. This triggers a configuration update to the phone and resolves the issue.
7894	Using the IP redirect feature, the deskphone does not display the correct redirect server URL during the bootup sequence. The deskphone shows the original server UR instead.
9477	If Audio report feature is active, the phone responds slowly for a few seconds until the report is complete.

ID	Issue Description
6339	In case the phone backup file is manually removed from the backup server, and then the phone reboots, the next backup operation would backup default parameters only. **Solution**: To ensure that the backup operation uses the correct backup parameters, do not remove the phone backup file from the backup servers manually
7131	In a Call Center, switching audio devices (handset, headset or speaker) while agent greeting is being played causes the agent greeting to stop. **Solution**: Do not switch audio devices while the greeting is being played.
8892	Call Center: When CALLCTRSTAT is 1 and agent is logged in, the value of HEADSYS will always be treated as 1.
7474	If OPSTAT is 00x or 0, OPTSTATCC and CALLCTRSTAT are set to 1, Advanced options functionality is not blocked.
7040	When 'Timerstat' is set to 1 and 'Timer on' softkey is chosen while on an active call, the user timer blinks when the seconds advance. **Solution:** Use 'Timer on' softkey during idle state (not during an active call).
5782	If a phone is ringing while a failover between primary and secondary CMs in a Processor Ethernet duplicate setup occurs, the ringing for the current call will stop. The phone will keep alerting silently until the call is answered or disconnected. The ringing will continue to function properly in the next call.
5078	If the HTTP server is down, and the user is registered by static IP address and modifies call server IP address, changes are not reflected on the phone. **Solution**: Verify that the HTTP server is up and running before making administrative changes.
4505	Arabic language is not supported on the 9608 desk phones.
5697	After performing a downgrade of software, changing CM configuration of Button Module parameters and then upgrading again, labels are not updated on Button Module. **Solution**: Perform a "CLEAR" operation.
7143	If you press a second call appearance while an auto answer greeting is being played, you hear the dial tone and the greeting at the same time.
8872	If you use barge-in audio push after normal audio push, the deskphone may reset.
8902	Phone does not support using DNS for WML host name or trusted push server **Solution**: Use IP address for WML host name or TPS host name.
8812	When several certificates are provided and the first is invalid, phone will not continue to download other certificate. **Solution**: Use valid certificates.
9582	Team button alert is shorter when using headset.
9500	In Hebrew or Arabic, the "Enter" and "Bksp" soft keys are switched on VPN startup. **Solution**: When using those system languages, after entering a password, press "Bksp" to Enter and vice versa.
9525	The agent greeting feature (including agent greeting recording) does not function with Bluetooth headsets. Only wired or DECT headsets are supported.

ID	Issue Description
9503	When setting the Log to file parameter at the CRAFT menu to ON and changing the Serial Port to "CLI", SBM button modules stop working. **Solution**: Change "Serial Port" back to "Adjunct" once debugging is completed. You can do this through the craft menu. Note: The DEBUG option is available for use only if you change the default password to the craft menu through the PROCPSWD parameter. The new value of the PROCPSWD parameter must be 4 to 7 numeric digits, "0000" through "9999999". However if value of PROCPSWD is less than 4 digits after you install R6.2.4 or later, the value will be changed back to the default value of 27238.
9586	The deskphone does not support WML of Push display when its title contains "&" or "<".
10033	After playing an existing greeting and using the RESTART soft key to re-record the greeting, the agent greeting icon will not be updated. **Solution**: Go to agent greeting screen and play one of the greetings. The icon will be updated correctly from this point on.
5870	When moving between states "After call" and "Auto-in", an Incorrect status line information appears. This problem is observed on 9611G phones only. **Solution**: Change the extension's configuration on CM to be administered as a 9650. CM Fixes (MR defsw100727) were delivered to the following releases: CM 6.0.1 SP04.00 CM 5.2.1 SP10.00
8533	Synchronization issue between phone and agent after a network outage that causes phone reset and login, causing audio issues when answering a call **Solution**: Communication Manager Fixes (MR defsw113036) were delivered in the following releases: 5.2.1sp14.00 6.0.1sp10.00 6.2sp00.00 cm6.3 base *Synchronization issue is that the device chosen (speaker/headset/handset) is not synchronized. Choosing that device several times will cause synchronization.
9559	When running against specific versions of CM - the Auto-In LED remains lit on phone after failover from Main to ESS **Solution**: Upgrade to CM version 6.2 FP2/3 or CM 6.0.1 SP 10.
9667	Phone supports getting only one HTTP file server from LLDP. **Solution**: Multiple HTTP file servers can be configured using other ways such as settings file, DHCP and CRAFT menu.
9771	For 9608 and 9611, in guest login screen, the softkeys will disappear after 2 wrong login attempts. This will prevent users from trying a third time. **Solution**: Press the "OK" key on the phone and the password field will appear. Enter the correct password and press the "Up" arrow button. All the keys will appear on the screen.
8897	If the phone is connected to the network using VPN, the BRURI parameter

ID	Issue Description
	contains FQDN address and not the IP address, and the phone is logged out and sleep mode is activated, backup/restore will stop working until the next phone reboot. **Solution**: Configure IP and not FQDN when the phone is behind VPN.

Appendix 1 – Supported Hardware

H.323 6.6.0 software is supported on the following models of IP Deskphones.

Comcode	Short Description	Model	Note
700480585	9608	9608D01A	
700504844	9608 GLOBAL	9608D02A	
		9608D02B	***Must use SIP 6.3.1.13 or later, or H.323 6.3.1.16 or later.***
700501428	9608 (TAA)	9608D02A	
700507947	9608 GLOBAL (TAA)	9608D02B	***Must use SIP 6.3.1.13 or later, or H.323 6.3.1.16 or later.***
700505424	9608G	9608D03A	***Must use SIP 6.3.1.13 or later, or H.323 6.3.1.16 or later.***
700480593	9611G	9611GD01A	
700501429	9611G (TAA)	9611GD01A	
700504845	9611G GLOBAL	9611GD02A	
		9611GD02B	***Must use SIP 6.4.0.33 or later, or H.323 6.4.0.14 or later.***
700507948	9611G GLOBAL (TAA)	9611GD02B	***Must use SIP 6.4.0.33 or later, or H.323 6.4.0.14 or later.***
700480601	9621G	9621GD01A 9621GD01C	
700506514	9621G GLOBAL	9621GD01C	
700500254	9621G (TAA)	9621GD01A 9621GD01C	
700506516	9621G GLOBAL (TAA)	9621GD01C	
700480619	9621G W/O FACEPLATE	9621GD01B 9621GD01D	
700480627	9641G	9641GD01A 9641GD01C	
700506517	9641G GLOBAL	9641GD01C	
700501431	9641G (TAA)	9641GD01A 9641GD01C	
700506519	9641G GLOBAL (TAA)	9641GD01C	
700480635	9641G W/O FACEPLATE	9641GD01B 9641GD01D	
700505992	9641GS GLOBAL	9641GD03A	***Must use SIP 6.5.0.17 or later, or H.323 6.6.0.25 or later.***
700509409	9641GS GLOBAL (TAA)	9641GD03A	
700509981	9641GS GLOBAL W/O FACEPLATE	9641GD03B	

Appendix 2 – Release History

The following table provides a history of the H323 6.2.x/6.3.x/6.4.x/6.6.x software releases. The "ID" column shows the identifier of this software which is seen on the "About Avaya one-X" or "About Avaya IP Deskphone" menu item.

Release	ID	Date	Link to Readme file
6.2.0	6.2009	February 2012	http://support.avaya.com/css/P8/documents/100157541
6.2.1	6.2119	June 2012	http://support.avaya.com/css/P8/documents/100162786
6.2.2	6.2209	July 2012	http://support.avaya.com/css/P8/documents/100165091
6.2.3	6.2312	January 2013	http://support.avaya.com/css/P8/documents/100169016
6.2.4	6.2408	May 2013	http://support.avaya.com/css/P8/documents/100172170
6.3.0	6.3037	August 2013	http://support.avaya.com/css/P8/documents/100174163
6.3.1	6.3116	January 2014	http://support.avaya.com/css/P8/documents/100177992
6.4.0	6.4014	June 2014	http://support.avaya.com/css/P8/documents/100180543
6.6.0	6.6028	April 2015	http://support.avaya.com/css/P8/documents/101009359

Appendix 3 – New 46xxsettings.txt parameters

The following new system parameters are added to the list of 9600 Series H.323 customizable system parameters:

Parameter name	Default Value	Possible values	Description
FIPS_ENABLED	0	0-1	Specifies whether only FIPS-approved cryptographic algorithms will be supported.
OCSP_ENABLED	0	0-1	Specifies whether OCSP will be used to check the revocation status of certificates. When OCSP is enabled, then OCSP will be used to check revocation status for the certificates presented by peers for any TLS connection (HTTPS, 802.1x with EAP-TLS, SLA Mon agent, IPSec VPN, SSO).
OCSP_ACCEPT_UNK	1	0-1	Specifies whether in cases where certificate revocation status for a specific certificate cannot be determined to bypass certificate revocation operation for this certificate.
OCSP_NONCE	1	0-1	Specifies whether a nonce will be included in OCSP requests and expected in OCSP responses.
OCSP_URI	""	0 to 255 ASCII characters - zero or one URI	Specifies a URI for an OCSP responder. The URI can be an IP address or hostname.
OCSP_URI_PREF	1	1-2	Specifies the preferred URI to use for OCSP requests if more than one is available.
OCSP_TRUSTCERTS	""	0 to 255 ASCII characters: zero or more file names or URLs, separated by commas without any intervening spaces	Specifies list of OCSP trusted certificates which are used as OCSP signing authority for the certificate that its revocation status is being checked. This is needed in case the OCSP responder uses a

			different CA than the root CA of the certificate that its revocation status is being checked.
SERVER_CERT_RECHECK_HOURS	24	0-32767	Specifies the number of hours after which certificate expiration and OCSP will be used (if OCSP is enabled) to recheck the revocation and expiration status of the certificates that were used to establish a TLS connection. A value of 0 means that periodic checks will not be done.
TLSSRVRVERIFYID	0	0-1	Specifies whether the identity of a TLS server is checked against its certificate. This parameter obsoletes TLSSRVRID.
CERT_WARNING_DAYS	60	0..99	Specifies how many days before the expiration of a certificate that a warning should first appear on the phone screen. Log and syslog message will be generated as well. The warning will reappear every 7 days.
PKCS12URL	""	0 to 255 ASCII characters, zero or one URL. The value must be a string that contains either "$SERIALNO" (which will be replaced by the telephone's serial number) or "$MACADDR" (which will be replaced by the telephone's MAC address), but it may contain other characters as well. The MACADDR used for PKCS12URL shall be without colons (i.e., 6 pairs of	Specifies the URL to be used to download a PKCS #12 file containing an identity certificate and its private key.

		ASCII hexadecimal characters aabbccddeeff with hex characters A-F encoded as upper-case characters).	
TLS_SECURE_RENEG	0	0-1	Specifies whether a TLS session will be terminated if the peer does not support secure renegotiation.
VLANSEPMODE	0	0-1	Specifies whether full VLAN separation between PC and phone's network ports is enabled. In this mode, tagged and untagged packets from PC port will never reach phone's port.
ENHDIALSTAT	1 for 9600	0-2	Specifies whether enhanced local dialing rules: Values: 0 - disabled. 1 - Enabled (for call history, web pages, but NOT for contacts) 2 - Enabled for all applications including contacts. Value 2 is NEW in this release.
MYCERTKEYUSAGE	""	0 to 255 ASCII characters. List of text strings, separated by commas without any intervening spaces, that will be compared to the values specified for the X.509 KeyUsage extension in Section 8.2.2.3 of X.509-2000 and for each matching value, the corresponding bit will be set in the SCEP PKCSReq; invalid strings will	Specifies the purpose(s) for which a certificate is issued.

		be ignored; Possible values are: "digitalSignature", "nonRepudiation", "keyEncipherment", "dataEncipherment", "keyAgreement", "keyCertSign", "cRLSign", "encipherOnly", "decipherOnly"	
VPNALLOWTAGS	0	0-1	Specifies specify whether 802.1Q can be enabled when VPN mode is active.
PHY2TAGS	0	0-1	Specifies whether to remove VLAN tags from frames forwarded to PC port (0) or not (1)
UDT	10	10-960	Specifies the Unsuccessful Discovery Timer (UDT) in minutes.
CADISPMODE	0	0-2	Specifies whether to add prefix in full width screen or prefix on the left column and suffix on the right column in half width screen. The prefix or suffix is ("a."-"z." lowercase and then "A."-"Z.) according to the button index and they will be added to all line/bridge appearances buttons labels. Values: 0 – Labels is changed according to call state where CM provides the labels. This is the behavior in pre 6.6 releases. 1 - Add ("a."-"z." lowercase and then "A."-"Z.) as described above. Value 2 – Do not add ("a."-"z." lowercase and then "A."-"Z.), but the label keeps the line/bridge appearance fixed and independent on call states.

CALLAPPRSELMODE	0	0-1	Controls highlight of call appearance when there is incoming call. Values: 0 – When there is incoming call, the call appearance of incoming call is highlighted and applicable softkeys are presented for incoming call ("Answer", "Ignore" if no other call exists or "Ans Hold", "Ans Drop", "Ignore" if another call exists). 1 – When there is incoming call, the highlight remains on the active/hold call appearance
CCBTNSTAT	1	0-1	Call Center softkey button permission flag. Values: 1 - Hold, Conference, Transfer and Drop softkey buttons are supported as in pre-6.6 release. 0 - Hold, Conference, Transfer and Drop softkey buttons are controlled by HOLDSTAT, CONFSTAT, XFERSTAT and DROPSTAT configuration parameters.
CONFSTAT	1	0-1	Conference SK button permission flag in call center environment. Values: 1 - Conference softkey button is supported as in pre-6.6 release. 0 - Conference softkey button is not presented.
DROPSTAT	1	0-1	Drop SK button permission flag in call center environment. Values: 1 – Drop softkey button is supported as in pre-6.6 release. 0 - Drop softkey button is

			not presented.
HOLDSTAT	1	0-1	Hold SK button permission flag in call center environment. Values: 1 - Hold softkey button is supported as in pre-6.6 release. 0 - Hold softkey button is not presented.
XFERSTAT	1	0-1	Transfer SK button permission flag in call center environment. Values: 1 – Transfer softkey button is supported as in pre-6.6 release. 0 - Transfer softkey button is not presented.
AGTCAINFOLINE	1	0-1	Controls presentation of call associated information in the agent information line. Values: 0 - The Agent Information Line presents agent-oriented information 1 - The Agent Information Line presents agent-oriented information as well call associated information (as supported in pre 6.6 releases).

License Agreements

The H.323 6.6 Third Party Terms document is available under the following path:

https://support.avaya.com/helpcenter/getGenericDetails?detailId=C200922314304731046

(Please scroll to the 96x1 H.323 section).