Avaya Deskphone SIP Release 7.1.6.0 Readme

This file is the Readme for the Avaya Deskphone SIP Release 7.1.6.0 software. This file describes the contents of the July 2019 (**7.1.6.0.8**) release software distribution package.

Avaya Deskphone SIP Release 7.1.6.0 software is supported on the Avaya 9601, 9608, 9608G, 9611G, 9621G, 9641G, and 9641GS IP Deskphones used with Avaya Aura® Communication Manager with Avaya Aura® Session Manager. Avaya Deskphone SIP Release 7.1.6.0 software is also supported on the Avaya 9601, 9608, 9608G, 9611G, 9621G, 9641G, and 9641GS IP Deskphones used with Avaya IP Office™ in a Centralized Branch configuration. The Avaya Deskphone SIP Release 7.1.6.0 software will not load or operate on any other models.

This release supersedes all previous Avaya Deskphone SIP 6.x/7.x software releases. Avaya recommends that all customers using Avaya Deskphone SIP 6.x/7.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.

Compatibility

The Avaya 9601, 9608, 9608G, 9611G, 9621G, 9641G, and 9641GS IP Deskphones using Avaya Deskphone SIP Release 7.1.5.0 software are supported on:

- Avaya Aura® Platform 7.0.0.0 (Avaya Aura® Communication Manager 7.0.0.0, Avaya Aura® Session Manager 7.0.0.0, Avaya Aura® System Manager 7.0.0.0) and associated service packs
- Avaya Aura® Platform 7.0.1.0 (Avaya Aura® Communication Manager 7.0.1.0, Avaya Aura® Session Manager 7.0.1.0, Avaya Aura® System Manager 7.0.1.0, Avaya Aura® Presence Services 7.0.1.0) and associated service packs
- Avaya Aura® Platform 7.1.0.0 (Avaya Aura® Communication Manager 7.1.0.0, Avaya Aura® Session Manager 7.1.0.0, Avaya Aura® System Manager 7.1.0.0, Avaya Aura® Presence Services 7.1.0.0) and associated feature/service packs
- Avaya Aura® Platform 8.0.0.0 (Avaya Aura® Communication Manager 8.0.0.0, Avaya Aura® Session Manager 8.0.0.0, Avaya Aura® System Manager 8.0.0.0, Avaya Aura® Presence Services 8.0.0.0) and associated feature/service packs
- Avaya Aura® Platform 8.0.0.0 (Avaya Aura® Communication Manager 8.1.0.0, Avaya Aura® Session Manager 8.1.0.0, Avaya Aura® System Manager 8.1.0.0, Avaya Aura® Presence Services 8.1.0.0) and associated feature/service packs
- Avaya Aura® Call Center Elite 7.0.1.0[1], 7.1.0.0[1], 8.0.0.0[1]
- IP Office™ 10.0 SP7 / 10.1 SP3 when deployed in a Centralized Branch configuration
- IP Office™ 11.0 and associated feature/service packs when deployed in a Centralized Branch configuration
- Avaya Aura® Application Server 5300 (AS5300) Release 3.0 SP13 and later

New Features in SIP 7.1.6.0

Avaya Deskphone SIP Release 7.1.6.0 contains the following new feature.

New with this release	Description
Avaya Acoustic Edge with Avaya L100 headsets	Avaya Acoustic Edge dynamically adjusts the received audio volume over extended period of time to not exceed government legislation for long-term acoustic exposure. **NOTE: *Only supported on 9608GD03B/9611GD02C hardware.***

Documentation for SIP 7.1.6.0

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

- Installing and Administering Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP
- Avaya 9600 Series IP Deskphones Overview and Specification
- Using Avaya 9601 IP Deskphone SIP
- Avaya 9601 IP Deskphone SIP Quick Reference
- Using Avaya 9608/9608G/9611G IP Deskphones SIP
- Avaya 9608/9608G/9611G IP Deskphones SIP Quick Reference
- Using Avaya 9621G/9641G/9641GS IP Deskphones SIP
- Avaya 9621G/9641G/9641GS IP Deskphones SIP Quick Reference
- Using Avaya 9608/9608G/9611G IP Deskphones SIP for Call Center Agents
- Using Avaya 9621G/9641G/9641GS IP Deskphones SIP for Call Center Agents
- Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP for Call Center Agents Quick Reference
- Guide to Icons – Avaya 9608/9608G/9611G/9621G/9641G IP Deskphones
- Implementing End-to-End SIP Vol 1: Endpoint Deployment
- Implementing End-to-End SIP Vol 2: SIP Telephone Signaling and Dial Plan Options
- White Paper for Avaya Aura® Dial Plan Processing by SIP Phones
- Avaya Aura® Multi-Device Access White Paper
- Avaya Deskphone H.323/SIP for 9600 Series – API Guide
- Application Note: EAP-TLS with 9600 Phones
- Avaya 96XX Series IP Deskphone and H100 Video Collaboration Station Headset Profiles

These documents are available on http://support.avaya.com under "9600 Series IP Deskphones" -> "SIP 7.1.x" -> Documents

SIP 7.1.6.0 (7.1.6.0.8) Package Content

The SIP 7.1.6.0 package (96x1-IPT-SIP-R7_1_6_0-062519.zip) contains all the files necessary to upgrade Avaya new or previously installed Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones to the SIP 7.1.6.0 software.

- S96x1_SALBR7_1_6_0r8_V4r83.tar – The SIP 7.1.6.0 application upgrade tar file.
- S96x1_UKR_V43r3642_V43r3642.tar– The SIP 7.1.6.0 platform system tar file.
- S9608_11_SALKRR7_1_6_0r8.bin – The SIP 7.1.6.0 application binary file.
- 96x1Supgrade.txt – The SIP 7.1.6.0 application upgrade file.
- Fifteen predefined language files plus Large English file for phone display:
    - Mlf_Arabic.xml
    - Mlf_BrazilianPortuguese.xml
    - Mlf_CanadianFrench.xml
    - Mlf_CastilianSpanish.xml
    - Mlf_Chinese.xml
    - Mlf_Dutch.xml
    - Mlf_Englarge.xml
    - Mlf_English.xml
    - Mlf_German.xml
    - Mlf_Hebrew.xml
    - Mlf_Italian.xml
    - Mlf_Japanese.xml
    - Mlf_Korean.xml
    - Mlf_LatinAmericanSpanish.xml
    - Mlf_ParisianFrench.xml
    - Mlf_Russian.xml
- Eight extended Korean ring tone files:
    - KoreanRT1.xml
    - KoreanRT2.xml
    - KoreanRT3.xml
    - KoreanRT4.xml
    - KoreanRT5.xml
    - KoreanRT6.xml
    - KoreanRT7.xml
    - KoreanRT8.xml
- One certificate file:
    - av_prca_pem_2033.txt – Avaya Product Root CA certificate with an expiration date of 2033
- Avaya-SparkIPTelephone-MIB.mib – mib file
- release.xml
- A "signatures" subdirectory containing signature files and a certificate file. Both SHA-1 and SHA-256 signature files are included
- Avaya Global Software License Terms 092018.pdf

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.**

Advisements with SIP 7.1.6.0 software

Limitations with IPv6

Deskphone SIP 7.1.1.0 and later includes initial support for IPv6 interworking. The following are known limitations of the current implementation:

- Deskphones cannot assign their own IP address (SLAAC). Only DHCPv6 is supported.
- Deskphones cannot resolve domain names into IPv6 addresses (AAAA records). As a result, a FQDN cannot be used for server configurations.
- Extended rebind is not supported.
- HTTP/HTTPS over IPv6 is not supported. The deskphones must use HTTP/HTTPS over IPv4 to retrieve settings files, software files, audio files, and language files.
- The following functionality is only supported via IPv4
    - RTCP
    - WML and Push
    - Microsoft Exchange integration
    - SNTP
    - Syslog (In addition, the syslog file will not show IPv6 addresses)
    - SCEP
    - Avaya Diagnostic Server (ADS / SLAMon)
    - SSH / Telnet (used only by Avaya Support)
    - SNMP
    - Shared Control / Deskphone Mode
    - Interworking with CC Elite.
- FQDN cannot be used for server configuration

As a result of these limitations, deskphones will only be supported in a mixed IPv4/IPv6 environment.

MAC Address based settings file provisioning

Deskphone SIP 7.1.1.0 and later adds the ability to use a unique provisioning file based upon the MAC address of the deskphone. When configured, the deskphone will request a provisioning file based upon it's MAC address.

To implement this mechanism, the following line must be added to the normal 46xxsettings.txt file:

GET $MACADDR.txt

The deskphone will subsequently request a file corresponding to it's MAC address. If the MAC address is 64C3549ACD1F, it will request a 64C3549ACD1F.txt file from the provisioning server.

Within that MAC provisioning file, the FORCE_SIP_USERNAME and FORCE_SIP_PASSWORD parameters can be used to automatically force that deskphone to log in to the provided username / password.

SSH – Remote Access (ASG/EASG)

Deskphone SIP software contains an SSH server which is used by Avaya Services only for debugging purposes. The SSH server supports only Avaya Services Logins ("craft" and "sroot"). By enabling Avaya Services Logins, you are granting Avaya access to your system. This is required to maximize the performance and value of your Avaya support entitlements by allowing Avaya to resolve product issues in a timely manner. By disabling Avaya Services Logins, you are preventing Avaya access to your system. This is not recommended as it can impact Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Services Logins should not be disabled. The access to the SSH server is protected by ASG (Legacy authentication algorithm) or EASG (new authentication algorithm). Enhanced Access Security Gateway (EASG) provides a more secure authentication compared to ASG for SSH server access. Deskphone SIP 7.1.0.0 and later software includes support for EASG and has removed ASG.

Deskphone SIP 7.1.1.0 added an admin menu item to clear SSH lockout which has occurred due to to many failed login attempts.

Support for SHA2-signed software files

As part of the security enhancements in Deskphone SIP 7.1.0.0 or later software, the software files are signed using both SHA-1 and SHA-256 digital signatures. Deskphone SIP 7.1.0.0 software is capable of SHA-1 and SHA-256 digital signature verification. Deskphone SIP 7.0.0.x and earlier software files are signed using SHA-1 digital signatures only and capable of SHA-1 digital signature verification only.

Complex Station Access Code and changes to CRAFT access

As part of the security enhancments introduced with Deskphone SIP 7.1.0.0, support has been added for complex administrator passwords. As part of this change, the use of a "Mute"+"CRAFT" key sequence is no longer supported. An "Admin" softkey has been added to the startup screen and login screen. An "Administration…" menu item has also been added in the "Options & Settings" screen. Using either the "Admin" softkey or the "Administration.." menu item results in prompting the user for the Administrator password.

Removal of Avaya SIP Root CA Certificate

As of Deskphone SIP 7.1.0.0, the Avaya SIP Root CA Certificate (av_sipca_pem_2027.txt) is no longer included in the installation package.

Support for OCSP

Deskphone SIP 7.1.0.0 and later software supports OCSP (Online Certficate 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 an ongoing TLS connection). OCSP is supported for 802.1x (EAP-TLS), SIP over TLS, and HTTPS.

FIPS 140-2 Cryptographic libaries

Deskphone SIP 7.1.0.0 and later software supports an administrator-configurable option to utilize FIPS 140-2 certified algorithms for cryptographic operations. 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
- SIP signaling over TLS
- SRTP
- Downloads over HTTPS of settings, upgrade files, trusted certificates, and PKCS#12 files (Note that TLSSRVR must be set and HTTPSRVR must be empty)
- OCSP

Microsoft Exchange integration uses a non-certified algorithm and must be disabled.

MLPP – Limitations during a server failure

Call override/preemption is not available during a preserved call caused by inability to access Session Manager.

Downgrade to 6.5.0 or earlier releases – disable 802.1x, re-enter passwords

In the event that an IP Deskphone has been upgraded to Deskphone SIP 7.0.0 or later software and must be downgraded to a Deskphone SIP 6.5.0 or earlier software, please note the following:

Prior to downgrading from Deskphone SIP 7.0 and later to Deskphone SIP 6.5.0 or earlier, customers **MUST** disable 802.1x on the associated data switch *before the downgrade. Failure to disable 802.1x will result in the deskphone not completing the downgrade and being in a non-service state.*

Deskphone SIP 7.0 and later software changes the way that passwords are stored internally to the IP Deskphone in order to increase security. Since Deskphone SIP 6.5.0 or earlier software does not incorporate the same changes, then downgrading an IP Deskphone to those releases will result in the password no longer working and the **passwords will have to be re-entered to restore operation**. This applies to the login password, 802.1X EAP-MD5 password, 802.1x EAP-TLS certificate password, and Microsoft Exchange password. Following the downgrade, when re-enabling EAP-MD5/TLS on the network, you will need to need to re-enter the password / re-download a new client certificate

SIP 7.0 and later – deprecation of SECURECALL

Deskphone SIP 6.2 introduced the ability to provide a visual indicator if SRTP is being used by the use of a SECURECALL setting. With the introduction of support in SIP 7.0 for an indicator under control of Avaya Aura® Platform 7.0, the previous feature has been deprecated. **Customers using SIP 7.0 on earlier versions of Avaya Aura® Platform will no longer see the visual indicator if SECURECALL is configured in their settings file.**

Bi-Directional EHS – Compatible Headsets

Compatibility testing of the Bi-Directional EHS functionality with headsets from 3rd-party vendors is undertaken through the Avaya DevConnect program.

9641G/9641GS - Bluetooth – Compatible Headsets

Compatibility testing of the 9641G/9641GS with Bluetooth headsets from 3rd-party vendors is undertaken through the Avaya DevConnect program.

9601 Global – Minimum Software Release

The 9601 SIP Deskphone Global (Comcode 700506783, Model ID 9601D01B) must use Deskphone SIP 6.3.1.21 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 IP Deskphones, it is recommended to use a mechanism to differentiate the software loads such as different HTTP servers or different GROUPs.

9611G Global – Minimum Software Release

The 9611G IP Deskphone Global (Comcode 700504845/700501429, Model ID 9611GD02B) must use either Deskphone SIP 6.4.0.33 or later software or Deskphone H.323 6.4.0.14 or later software.

The 9611G IP Deskphone Global (Comcode 700504845/700501429, Model ID 9611GD02C) must use either Deskphone SIP 7.0.1.0.45 or later software or Deskphone H.323 6.6.2.29 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 IP Deskphones, it is recommended to use a mechanism to differentiate the software loads such as different HTTP servers or different GROUPs.

9608G and 9608 Global – Minimum Software Release

The 9608G IP Deskphone (Comcode 700505992/700507946, Model ID 9608GD03A) and 9608 IP Deskphone Global (Comcode 700504844/700507947, Model ID 9608D02B) must use either Deskphone SIP 6.3.1.13 or later software or Deskphone H.323 6.3.1.16 or later software.

The 9608G IP Deskphone (Comcode 700505424/700507946, Model ID 9608GD03B) must use either Deskphone SIP 7.0.1.0.45 or later software or Deskphone H.323 6.6.2.29 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 IP Deskphones, it is recommended to use a mechanism to differentiate the software loads such as different HTTP servers or different GROUPs.

9641GS – Minimum Software Release

The 9641GS IP Deskphone (Comcode 700505992/700509409/700509981, Model ID 9641GD03A) must use either Deskphone SIP 6.5.0.17 or later software or Deskphone H.323 6.6.0.25 or later software.

The 9641GS IP Deskphone (Comcode 700505992/700509409/700509981, Model ID 9641GD03C) must use either Deskphone SIP 7.1.1.0.9 or later software or Deskphone H.323 6.6.6.04 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 IP Deskphones, it is recommended to use a mechanism to differentiate the software loads such as different HTTP servers or different GROUPs.

HEADSYS – Change in Default Parameter to 0

The HEADSYS parameter specifies whether the IP Deskphone will go on-hook if the headset is active when a Disconnect message is received. As of SIP 6.4.0, the default for this parameter has changed from 1 to 0. Customers who want to maintain the previous operation are advised to modify their settings file to specifically set the value of this parameter to 1.

Microsoft Exchange Integration using EWS

If Microsoft Exchange Integration is enabled and the phone is connecting to Exchange Server 2010 or later, Exchange Web Services (EWS) is used for the connection. This connection is secured using HTTPS by default which means that the phone is required to validate the Exchange Server identity certificate. To validate the certificate, the TRUSTCERTS parameter in the settings file must include the root certificate of the Certificate Authority (CA) which issued the Exchange Server identity certificate. This configuration will work if the identity certificate was directly issued by the CA root certificate.

If a public CA such as VeriSign is used to obtain an identity certificate for the Exchange Server, the identity certificate will be issued by an intermediate CA certificate and not by the root. In this case, both the root and intermediate CA certificates must be installed on the phone using TRUSTCERTS or the HTTPS connection will fail. In general, if the Exchange Server identity certificate is issued by an intermediate CA, all certificates from the intermediate CA up to the root must be included in TRUSTCERTS for installation on the phone so that the entire certificate chain is available for validation.

Avaya Presence Services - Instant Messaging (IM) and Presence

If IM is configured, it will be necessary to configure phones with the root CA certificate which issued an identity certificate to the Presence Server when it was installed. If SMGR was used to issue a certificate to the Presence Server, the root CA certificate can be obtained from SMGR under Services / Security / Certificates / Authority. Simply click on the "Download pem file" link and put the downloaded file on the http server in the same location as 46xxsettings.txt. Finally the following line needs to be added to the settings file (assuming the CA certificate filename is smgr_ca.txt).

```
SET TRUSTCERTS av_sipca_pem_2027.txt,smgr_ca.txt
```

Note: there must be no spaces in the certificate list

Instant Messaging is not supported when two sets are configured with the same extension via Multi Device Access (MDA).

Avaya Deskphone SIP Release 6.5.0 adds support for Presence Communications Profile which explicitly associates a user with an Avaya Aura® Presence Services (PS) server instance. If a Fully Qualified Domain Name (FQDN) is programmed via the Presence Communications Profile, the associated FQDN must be resolvable to the same IP address by both Avaya Aura® Session Manager (including via Local Host Name Resolution) and via Domain Name System (DNS) on the IP Deskphone. The IP address / FQDN received via this mechanism supersedes any PS IP address programmed in the 46xxsettings.txt file (via SET PRESENCE_SERVER).

To get Instant Messaging to work, as of 7.1.0.0, you have to set the following parameters:

1) If validation is not required then settings file should have

SET TLSSRVRID 0

2) If validation is required then settings file should have

SET TLSSRVRID 1 (this is the default value)

SET FQDN_IP_MAP "FQDN name=IP address"

Restriction on Busy Indicators on Button Modules:

- 3 button modules can be connected
- The IEEE power switch on the back of the 9608G deskphone must be set to "H" (high) when connecting one or more button modules.
- The maximum combined number of busy indicators, team buttons and bridged appearances that can be configured on button modules is **48**.
- All button module lines can be configured as long as the restriction above is met.

Debug mode

As a general guide, it should be noted that response times could be impacted when debug or syslog is enabled

Server setting precedence

When upgrading a 9608/9608G/9611G/9621G/9641G/9641GS SIP Deskphone from H.323 to SIP software please note that any setting that is set via the CRAFT menu (e.g. IP address) will take precedence over the information provided by DHCP when the phone is in SIP mode. For example if the HTTP server is set via that CRAFT menu in H.323 and then during the upgrade to SIP, if the phone requests new DHCP data, the DHCP data will not overwrite the data provided by the CRAFT menu.

SIP_CONTROLLER_LIST & SIP_CONTROLLER_LIST_2

This parameter consolidates SIP controller parameters for IP address, port, and transport protocol into a single configuration parameter. The parameter setting should be a list of controller information where the format for each controller entry is "host:port;transport=xxx" . The host should be specified only by an IP address. The use of Fully Qualified Doman Names (FQDN) is not supported. This applies to all sources of the SIP_CONTROLLER_LIST parameter which includes DHCP, LLDP, and the 46xxsettings.txt file.

Note: 7.1.5.0 will ignore FQDN entries in the sip controller lists.

SRTP (Media Encryption)

In order to correctly use SRTP, there are various components within the network that you must correctly configure. For 9600 Series IP Deskphones to function properly with SRTP, you must configure the equivalent parameters in Communication Manager or System Manager. Avaya strongly recommends that the following three parameters on the 9600 Series IP Deskphones and the equivalent Communication Manager parameters must match:

SET ENFORCE_SIPS_URI 1
SET SDPCAPNEG 1
SET MEDIAENCRYPTION X or
SET MEDIAENCRYPTION X,Y or
SET MEDIAENCRYPTION X,Y,Z

Deskphone SIP 7.0.0 and later support AES-256 media encryption. Care must be taken to properly configure the encryption parameter when this is used in conjunction with other devices that do not support AES-256.

EAP TLS

When EAP-TLS is enabled using the CRAFT menu, the phone should be rebooted to allow for proper EAP-TLS authentication.

Multi Device Access

Refer to the "Avaya Aura Multi Device Access White Paper" which is available on http://support.avaya.com for known limitations.

When using MDA, it is recommended that the associated station on Avaya Aura® Communication Manager be administered as a "9641SIP".

9601 & 9608 Language support

The 9601 and 9608 do not support Arabic.

The 9601 phone cannot display Korean symbols when the current language is Chinese/Hebrew/Japanese.
The 9608 phone cannot display Korean symbols when the current language is Chinese/Japanese.

9601 and Topline Displays

The 9601 SIP Deskphone has a smaller screen size than other models and will sometimes display less information than other models. As an example, users may not always get a count of current and total calendar reminders.

Ringtone and Ringtone Wave Files

Ringtone wave files should be placed in the root directory of the HTTPSRVR. Additionally, numeric only conventions should be avoided with ringtone names. The maximum allowed size of an individual ringtone file is 512 kb. The maximum allowed size of all ringtone files is 5120 kb.

Headset Profiles

Deskphone SIP 6.3.0 introduced "Headset Profiles" to provide optimum performance for different brands of headsets. An up-to-date version of the profile <-> vendor cross reference can be found at https://downloads.avaya.com/css/P8/documents/100173755.

Avaya Session Border Controller for Enterprise

For all IP Deskphones phones which are remotely connected through an SBCE, please ensure that the following is set in the 46xxsettings.txt file

```
SET WAIT_FOR_REGISTRATION_TIMER 40
```

The following features are not supported through SBCE:

- Exchange integration (Contact search and Calendar)
- Custom Applications in the Home menu
- Display Home Page when using the browser icon
- Report logs to a log file server.
- WML Browser
- WML Push

Support for more than one device registered with the same account outside of the SBCE requires the use of ASBCE Release 6.2.1 or later.

SIPS

If there are any SIP endpoints not upgraded to SIP 6.3.x or later (i.e. running SIP 6.2.2 or earlier), those endpoints not upgraded should not enable SIPS mode unless all endpoints in the system are configured to register over TLS. Otherwise, SIPS calls from these endpoints to a TCP registered phone will fail, as the SIPS registered endpoint will not retry the request. SIPS mode is configured using "SET ENFORCE_SIPS_URI 1" and SRTP is enabled in the MEDIAENCRYPTION setting. Note that for all endpoints running SIP 6.3 or later, this is not an issue as the endpoint will automatically retry failed calls.

SIP Transport Protocols

TCP or TLS are the recommended transport protocols. UDP transport is not supported with deskphone SIP software.

Encryption – SHA2 and RSA 2048

Avaya Deskphone SIP Release 6.4.0 and later software supports RSA 2048 bit length encryption keys and supports the SHA2 (224, 256, 384, and 512) hash algorithm. This has been certified for HTTPS usage for web-based administration of these phone sets. When the TLS server-client handshake is initiated, this IP Deskphone (operating as the client) is able to send its Identity certificate with an enhanced digital signature (SHA2/2048 key). Additionally, this IP Deskphone is able to receive and validate server Identity certificates which have an enhanced digital signature (SHA2/2048 key).

Interworking – Avaya Diagnostic Server (ADS)

Avaya Deskphone SIP Release 6.4.1 and later software includes an updated version of the SLAMon agent software (2.0). The SLMSRVR parameter must be set in the 46xxsettings.txt file for this version of the agent to register with ADS. In addition, a valid certificate file must be downloaded via TRUSTCERTS.

Avaya Deskphone SIP Release 7.0.0 and later software includes an updated version of the SLAMon agent software (2.5). Avaya Diagnostic Server 2.5 is required to support this version.

Avaya Diagnostice Server 2.5.3 is required to support Deskphone SIP Release 7.0.1.0 or later software.

"Desk Phone" Mode and Lock

Avaya one-X® Communicator, Avaya Equinox and similar UC applications from Avaya support a "Desk Phone" (Shared Control) mode in which the UC application can control an associated IP Deskphone. An IP Deskphone supports a "Lock" mode, which can be entered either manually or automatically, which prevents the dialing of any number except for an emergency number using the keypad of the IP Deskphone. If an IP Deskphone is in Shared Control with a UC application and is also in a "Lock" state, placing a call from the UC application will still result in the call being established from the IP Deskphone.

SCEP– upgrading with 1024 bit certificates

With Deskphone SIP Release 6.5.0 or later software, the default value of MYCERTKEYLEN has changed from 1024 to 2048. If a customer has previously used SCEP to install identity certificates but did NOT explicitly specify MYCERTKEYLEN in the settings file then it would have used the default of 1024. Once Deskphone SIP Release 6.5.0 or later is installed, the value of MYCERTKEYLEN will effectively change to 2048 causing phones to attempt to upgrade identity certificates (which will result in a longer boot cycle). If phones already have identity certificates installed with 1024 bit keys, customer should explicitly set MYCERTKEYLEN to 1024 in their settings file to avoid this occurrence.

Presence Services – presence status on Avaya one-X® Deskphone SIP 2.6

Avaya one-X® Deskphone SIP Release 6.5.0 or later software includes changes to the methodology used to publish an "On A Call" state. Avaya one-X® Deskphone SIP Release 2.6.14 or later is required in order to correctly display presence status on a 9600-Series IP Deskphone using Avaya one-X® Deskphone SIP 2.6.x software.

9601 - Aliasing

Avaya Aura® Communication Manager does not provide native support of the 9601 IP Deskphone. The 9601 SIP Deskphone should be administered as a "9608SIP".

Interworking – Prognosis – RTCP-XR

Avaya Deskphone SIP Release 7.0 software adds support for the reporting of RTCP-XR metrics to a configured RTCPMON server. Prognosis (https://www.devconnectmarketplace.com/ir/prognosis) from Integrated Research has added support for this capability. Until such a time as this capability is offered in a generally available offering, existing Prognosis customers can contact IR Prognosis (http://www.ir.com/contact-us) to request a consultant quote to add the RTCP-XR monitoring capability.

Upgrades – from H.323 6.0.x or SIP 6.0.x/6.1.x

When upgrading an IP Deskphone from Deskphone H.323 6.0.x software or Deskphone SIP 6.0.x/6.1.x software, a two-step upgrade process is required. These deskphones must first be upgraded to Deskphone SIP 6.2.0 software, and then upgraded to the required Deskphone SIP 6.x/7.x software.

Interworking – Session Manager 6.3.13 or later – minimum release of Deskphone SIP software

Due to the POODLE vulnerability (CVE-2014-3566), support for SSLv3 was removed from Avaya Aura® Session Manager in 6.3.13. Any endpoionts, clients, SIP trunk devices, and third-party applications that made use of SSLv3 for SIP or PPM-based communication with Session Manager will no longer function on Session Manager 6.3.13 or later. Support for SSL v3 was also removed from Deskphone SIP 6.5.0 software. As such, any customers using Deskphone SIP 6.x software MUST upgrade those deskphones to SIP 6.5.0 or later software PRIOR to upgrading a Session Manager implementation to 6.3.13 or later. Refer to PSN004487u for additional information.

Demo Certificates – Avaya Aura® Session Manager 6.3.8 and newer

New installations of Avaya Aura® Session Manager Release 6.3.8 and newer generate SIP and HTTPS (PPM) certificates signed by System Manager CA during installation. Previous versions used a demo Avaya certificate which is deprecated as it does not meet current NIST security standards. The generated Session Manager certificates signed by System Manager CA do not contain all the attributes (SIP domain, IP address, etc.) required by the Avaya Deskphone SIP to correctly validate them. For that reason it is recommended to replace them. To replace the Session Manager certificates signed by System Manager CA to comply with the SIP Deskphone requirements, follow the "Installing Enhanced Validation Certificates for Session Manager" section of the Session Manager Administration Guide. Optionally customers could replace the Session

Manager certificates for those signed by a third party CA. For more details, follow the Session Manager Administration Guide.
Upgrading to Avaya Aura® Session Manager Release 6.3.8 or later preserves the demo Avaya certificates used on SIP and HTTPS (PPM) TLS connections. It is highly recommended to replace the demo Avaya certificates. Refer to the Session Manager Administrator Guide for more details.

Security Certificates – IP Address versus FQDN

There is an industry movement towards the use of a FQDN (Fully Qualified Domain Name) instead of an IP address for the Subject Alternate Name or Subject Common Name for security certificates. Avaya Deskphone SIP Release 7.1.0.x or later software supports a FQDN_IP_MAP parameter which specifies mapping of FQDNs to IP addresses for the purpose of validating an FQDN identity found in a server certificate.

Interworking – Presence Services 7.0 or later – solution recovery

Please review to the Presence Services customer documentation (Avaya Aura® Presence Services Snap-in Reference Release 7.0) for the latest information related to the solution recovery mechanism used in Avaya Aura® Platform 7.0.
https://support.avaya.com/products/P0517/avaya-aura-presence-services/7.0.x

802.1x – Authentication

If the PC attached to the phone is not expected to use 802.1x authentication, then:

1) Disable any 802.1x supplicant on the PC

2) Disable the 802.1x "pass-thru" mode on the phone.

Otherwise, there is a possibility that during phone bootup, the PC may show a prompt to the user to enter 802.1x credentials.

Interworking – TLS 1.2

Deskphone SIP 7.0.1.0 and later software upgrades EAP-TLS to support TLS 1.2 and adds new cipher suites FIPS:!ADH:!DSS:-SSLv3:DHE-RSA-AES256-SHA:AES256-SHA:DHE-RSA-AES128-SHA:AES128-SHA.

Deskphone SIP 7.0.1.0 also adds a new configuration parameter (TLS_VERSION) which can be used to configure the Deskphone to only use TLS 1.2. Care must be taken to only use this parameter when all components to which the deskphone will communicate can also support TLS 1.2.

Interworking – HTTPS - MVIPTEL, IIS 6

Deskphone SIP 7.0.1.0 and later software does not support secure HTTP (HTTPS) with MVIPTEL or IIS 6. MVIPTEL is end-of-support by Avaya and IIS 6 is end-of-support by Microsoft. Customers using either of these servers are recommended to upgrade to a current version of an HTTPS server which supports TLS 1.2.

SIP 7.1.6.0 Resolved Issues (since SIP 7.1.5.0)

The following table includes issues which are resolved with this release of software compared to SIP 7.1.5.0.11

External ID	Internal ID	Issue Description
Audio		
User Interface		
1-14704139432	SIP96X1-56121	96x1 Do not apply BAKLIGHTOFF when not registered
1-14768688221	SIP96X1-59359	96x1 BA icons on phone mismatch SBM24
Avaya Aura®		
1-14701490462	SIP96X1-57660	96x1 Cannot transfer in shared control mode - only phone reboot solves issue
1-14755106602	SIP96X1-60179	Phone does not show VDN info when CM Agent has auto answer enabled
1-14651125166	SIP96X1-60054	Display issue when call picked up using FAC NOTE: Fix requires additional settings: **SET LOG_DIALED_DIGITS 0** **SET UPDATE_DIALED_NUMBER_ON_ANSWER 1**
Networking		
1-13894339072	SIP96X1-48843	multicast is not working or working very slowly

Unresolved issues in SIP 7.1.6.0

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

External ID	Internal ID	Issue Description
User Interface		
	SIP96X1-53059	Touch phone (9641/9621) cannot receive notification from ANS (Avaya Notification Server)
	SIP96X1-39931	9641G - Phone doesn't show Gateway IPV6 in ADDR and Network Information screen.
	SIP96X1-30070	9611/9608: Phone makes a call when pressing "More" SK in Calendar Exchange
	SIP96X1-60190	Phone generate core "MSM" when drop last participant in share control mode
Presence and IM		
	SIP96X1-40683	9621 - Phone does not receive Instant Message while user logged out in Automatic presence state and login
Networking		
	SIP96X1-26705	96x1 – Phone does not download trustcerts from second HTTP server which sets in settings file (SSON HTTPSRVR)
	SIP96X1-60153	Phone keeps old settings after clear in case phone is running in dual mode.

Appendix 1 – Supported Hardware

SIP 7.1.3.0 software is supported on the following models of IP Deskphones. All models except the 9601 ship pre-installed with H.323 software and must be upgraded to SIP 7.1.x as part of the installation process. The 9601 may not be shipped with SIP 7.1.x software and should also be upgraded to SIP 7.1.x as part of the installation process.

Note: Comcodes indicated with an asterisk (*) are either end-of-sale or pending end-of-sale and include a link to the corresponding end-of-sale document.

Comcode	Short Description	Model	Note
700500254*	9601	9601D01A	Ships with SIP software.
700506783*	9601 GLOBAL	9601D01B	Ships with SIP software. ***Must use SIP 6.3.1.21 or later.***
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 GLOBAL	9608GD03A	***Must use SIP 6.3.1.13 or later, or H.323 6.3.1.16 or later.***
		9608GD03B	***Must use SIP 7.0.1.0.46 or later, or H.323 6.6.2.29 or later.***
700507946*	9608G GLOBAL (TAA)	9608GD03A	***Must use SIP 6.3.1.13 or later, or H.323 6.3.1.16 or later.***
		9608GD03B	***Must use SIP 7.0.1.0.46 or later, or H.323 6.6.2.29 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.***
		9611GD02C	***Must use SIP 7.0.1.0.46 or later, or H.323 6.6.2.29 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.***
		9611GD02C	***Must use SIP 7.0.1.0.46 or later, or H.323 6.6.2.29 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)	9641GD03C	***Must use SIP 7.1.1.0.9 or later, or H.323 6.6.6.04 or later.***
700509409	9641GS GLOBAL (TAA)	9641GD03A	***Must use SIP 6.5.0.17 or later, or H.323 6.6.0.25 or later.***
		9641GD03C	***Must use SIP 7.1.1.0.9 or later, or H.323 6.6.6.04 or later.***
700509981	9641GS GLOBAL W/O FACEPLATE	9641GD03B	***Must use SIP 6.5.0.17 or later, or H.323 6.6.0.25 or later.***
		9641GD03D	***Must use SIP 7.1.1.0.9 or later, or H.323 6.6.6.04 or later.***

Appendix 2 – Release History

The following table provides a history of the SIP 6.2.x/6.3.x/6.4.x/6.5.x/7.x software releases. The "ID" column shows the identifier of this software which is seen on the "About Avaya one-X" or "About Avaya" menu item.

Release	ID	Date	Link to Readme file
6.2.0	6.2.0.72	August 2012	http://support.avaya.com/css/P8/documents/100165516
6.2.1	6.2.1.26	December 2012	http://support.avaya.com/css/P8/documents/100167697
6.2.2	6.2.2.17	July 2013	http://support.avaya.com/css/P8/documents/100170859
6.3.0	6.3.0.73	November 2013	http://support.avaya.com/css/P8/documents/100175296
6.3.1	6.3.1.13	January 2014	http://support.avaya.com/css/P8/documents/100177649
6.3.1 Up-issue	6.3.1.22	May 2014	http://support.avaya.com/css/P8/documents/100180124
6.4.0	6.4.0.33	June 2014	http://support.avaya.com/css/P8/documents/100179446
6.4.1	6.4.1.25	August 2014	http://support.avaya.com/css/P8/documents/100181857
6.5.0	6.5.0.17	January 2015	http://support.avaya.com/css/P8/documents/101004503
7.0.0	7.0.0.39	August 2015	http://support.avaya.com/css/P8/documents/101011869
7.0.1.0	7.0.1.0.46	May 2016	http://support.avaya.com/css/P8/documents/101023922
7.0.1.1	7.0.1.1.5	June 2016	http://support.avaya.com/css/P8/documents/101026740
7.0.1.2	7.0.1.2.9	September 2016	http://support.avaya.com/css/P8/documents/101027550
7.0.1.3	7.0.1.3.4	December 2016	http://support.avaya.com/css/P8/documents/101032198
7.0.1.4	7.0.1.4.6	February 2017	http://support.avaya.com/css/P8/documents/101034344
7.1.0.0	7.1.0.0.57	June 2017	http://support.avaya.com/css/P8/documents/101039138
7.1.0.1	7.1.0.1.1	July 2017	http://support.avaya.com/css/P8/documents/101041101
7.1.1.0	7.1.1.0.9	September 2017	http://support.avaya.com/css/P8/documents/101042670
7.1.2.0	7.1.2.0.14	May 2018	http://support.avaya.com/css/P8/documents/101048114
7.1.3.0	7.1.3.0.11	August 2018	http://support.avaya.com/css/P8/documents/101050791
7.1.4.0	7.1.4.0.11	December 2018	http://support.avaya.com/css/P8/documents/101054043
7.1.5.0	7.1.5.0.11	April 2019	http://support.avaya.com/css/P8/documents/101056710
7.1.6.0	7.1.6.0.8	July 2019	http://support.avaya.com/css/P8/documents/101058670

Appendix 3 – New and changed 46xxsettings.txt parameters

The latest version of the 46xxsettings.txt file can be downloaded from

https://support.avaya.com/downloads/download-details.action?contentId=C201773928555860_8&productId=P0553

Changed parameters.

New parameters.

```
## UPDATE_DIALED_NUMBER_ON_ANSWER specifies whether displayed dialed number is updated or not based
the number provided in 200 OK after an answer.
##  Value  Operation
##    0    Displayed dialed number is not updated based on 200 OK received after answer (default)
##    1    Displayed dialed number is updated based on the number provided in 200 OK after answer.
##  This parameter is supported by:
##       J100 SIP R4.0.2.0 and later
## SET UPDATE_DIALED_NUMBER_ON_ANSWER 1
```

License Agreements

License agreements are available at https://support.avaya.com/Copyright. Please select 96x1 SIP.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Documentation disclaimer.

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this Documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.