



Avaya J100 Series SIP Release 2.0.0.0 Readme

This file is the Readme for the Avaya J100 Series SIP Release 2.0.0.0 software (J100 SIP 2.0.0). This file describes the contents of the April 2018 (**2.0.0.0.45**) release software distribution package.

J100 SIP 2.0.0 software is supported on the Avaya J129, J169, and J179 IP Phones used with Avaya Aura®, Avaya IP Office™, and select 3PCC (3rd party call control platforms). J100 SIP 2.0.0 software will not load or operate on any other models.

This release supersedes all previous Avaya J100 Series SIP 1.x software releases. Avaya recommends that all customers using Avaya J100 Series SIP 1.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 J129, J169 and J179 IP Phones using J100 SIP 2.0.0 software is supported with:

- Avaya Aura® Platform 6.2 FP4 (Avaya Aura® Communication Manager 6.3.6, Avaya Aura® Session Manager 6.3.8, Avaya Aura® System Manager 6.3.8) and associated service packs
- 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) 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
- IP Office™ 10.0 SP2 or later (J129 only)
- IP Office™ 11.0 or later
- Avaya Aura® Call Center Elite 7.0.1.0¹, 7.1.0.0¹
- 3PCC (3rd party call control) Platform
 - Broadsoft Broadworks R21SP1
 - Zang Office R1.0
 - Edgewater Network device (Edgemarc 4550).

¹ J169/J179 IP Phone is supported with CC Elite. The J129 IP Phone is not supported with CC Elite.

New Features in J100 SIP 2.0.0

Avaya J100 Series SIP Release 2.0.0.0 contains the following new features

New with this release	Description
<p>New User Interface for J169/J179</p> 	<p>J100 Release 2.0 introduces a complete redesign of the User Interface for the J169/J179. A partial list of the new capabilities includes:</p> <ul style="list-style-type: none"> • Ability to customize the layout of the main screen as well as JBM24 screens • Addition of contact groups • Six built-in screen savers and six built-in background images with ability to import more • Expanded integration with Microsoft Exchange calendars including full month view • Updated interface for CC Elite • Variable font sizes for all languages
"Guest Login" for J169/J179	Users can temporarily log into an already-logged-in phone and it will reconfigure according to their saved parameters. On timeout or log out, the phone automatically reverts to the previous login/configuration.
Support for J100 Wireless Module	WLAN connectivity is available on the J129/J179 where wired Ethernet is not available. It requires an additional plug-in hardware module.
Web Administration 	J100 Release 2.0 software adds the ability to remotely access a J129/J169/J179 via a web browser and perform many of the functions which previously required physical access to the phone.
IP Office – improved interworking for J169/J179	In conjunction with IP Office 11.0, the SIP-based J169/J179 provides similar functionality to what is offered with an H.323-base 9611G IP Deskphone. For a full list of the supported functionality, refer to the IP Office documentation.
Remove audio brand	Administratable option to turn off the audio branding (played on logging in).
Save extension on log-out	Administratable option to autofill the previous logged-in user on the "User" log-in screen.
Voice Mail softkey (J129 only)	Administratable option to have the Voicemail key as one of the three softkeys that are present on the idle screen of the J129.
Support for DES (Device Enrollment Service)	DES is an Avaya-hosted server which provides the ability to redirect ex-factory IP Phones to a configuration server. For more details, refer to the DES Offer Definition/Documentation.
J169/J179 concurrency with J100 Release 1.0/1.1 software	<p>With SIP 2.0 software, the J169/J179 support:</p> <ul style="list-style-type: none"> • Opus codec • Interworking with select 3PCC • Handset profiles • Contact name format

New with this release	Description
J129 concurrency with J100 Release 1.5 software	With SIP 2.0 software, the J129 supports: <ul style="list-style-type: none">• FIPS 140-2• Display call forward from original dialed station• Support for dual-stack IPv4/IPv6

Documentation for J100 SIP 2.0.0.0

The following documentation has been provided for this release:

- [Avaya J100 Series IP Phone Overview and Specifications](#)
- [Installing and Administering Avaya J100 Series IP Phone](#)
- [Installing and Administering Avaya J100 series IP Phone in third-party call control setup](#)
- [Using Avaya J169/J179 IP Phone SIP in a Call Center](#)
- [Using Avaya J129 IP Phone SIP](#)
- [Using Avaya J129 IP Phone SIP in third party call control setup](#)
- [Avaya J129 IP Phone SIP Quick Reference](#)
- [Using Avaya J169/J179 IP Phone SIP](#)
- [Using Avaya J169/J179 IP Phone SIP in third-party call control setup](#)
- [Avaya J169/J179 IP Phone SIP Quick Reference](#)
- [Using Avaya JBM24 Button Module](#)

These documents are available on <http://support.avaya.com> under "J100 Series IP Phones "
-> "SIP 2.0.x" -> Documents

J100 SIP 2.0.0.0 (2.0.0.0.45) Package Content

The J100 SIP 2.0.0.0 (J100-IPT-SIP-R2_0_0_0-040718.zip) contains all the files necessary to upgrade Avaya new or previously installed Avaya J129/J169/J179 IP Phones to the J100 SIP 2.0.0.0 software.

- FW_S_J129_R2_0_0_0_45.bin – application binary file for J129
- FW_S_J169_R2_0_0_0_45.bin – application binary file for J169
- FW_S_J179_R2_0_0_0_45.bin – application binary file for J179
- J100Upgrade.txt – This file is downloaded by the IP Phones and instructs the phone on how to upgrade to this version of software
- Predefined language files for phone display:
 - Mlf_J129_BrazilianPortuguese.xml
 - Mlf_J129_CanadianFrench.xml
 - Mlf_J129_CastilianSpanish.xml
 - Mlf_J129_Chinese.xml
 - Mlf_J129_Dutch.xml
 - Mlf_J129_English.xml
 - Mlf_J129_German.xml
 - Mlf_J129_Hebrew.xml
 - Mlf_J129_Italian.xml
 - Mlf_J129_Japanese.xml
 - Mlf_J129_Korean.xml
 - Mlf_J129_LatinAmericanSpanish.xml
 - Mlf_J129_ParisianFrench.xml
 - Mlf_J129_Polish.xml
 - Mlf_J129_Russian.xml
 - Mlf_J129_Turkish.xml
 - Mlf_J169_J179_Arabic.xml
 - Mlf_J169_J179_BrazilianPortuguese.xml
 - Mlf_J169_J179_CanadianFrench.xml
 - Mlf_J169_J179_CastilianSpanish.xml
 - Mlf_J169_J179_Chinese.xml
 - Mlf_J169_J179_Dutch.xml
 - Mlf_J169_J179_English.xml
 - Mlf_J169_J179_German.xml
 - Mlf_J169_J179_Hebrew.xml
 - Mlf_J169_J179_Italian.xml
 - Mlf_J169_J179_Japanese.xml
 - Mlf_J169_J179_Korean.xml
 - Mlf_J169_J179_LatinAmericanSpanish.xml
 - Mlf_J169_J179_ParisianFrench.xml
 - Mlf_J169_J179_Polish.xml
 - Mlf_J169_J179_Russian.xml
 - Mlf_J169_J179_Thai.xml
 - Mlf_J169_J179_Turkish.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-J100iPhone-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 102016v1.pdf

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

Advisements with J100 SIP 2.0.0.0 software

J169/J179 – Upgrade from J100 SIP 1.5.0 – re-enter configuration



End-users who have customized their J169/J179 when using J100 SIP 1.5.0 software will need to re-do the customization following an upgrade to J100 SIP 2.0.0

Limitations with IPv6

J100 1.5.0 and later includes 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
 - 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.

SSH – Remote Access (EASG)

J100 SIP software contains an SSH server which is used only by Avaya Services 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 EASG (Enhanced Access Security Gateway).

Support for SHA2-signed software files

The software files are signed using both SHA-1 and SHA-256 digital signatures. J100 SIP software is capable of SHA-1 and SHA-256 digital signature verification.

Removal of Avaya SIP Root CA Certificate

The Avaya SIP Root CA Certificate (av_sipca_pem_2027.txt) is not included in the installation package.

Support for OCSP

J100 SIP software supports 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 an ongoing TLS connection). OCSP is supported for 802.1x (EAP-TLS), SIP over TLS, and HTTPS.

FIPS 140-2 Cryptographic libraries

J100 SIP 1.5.0 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 TLSSRV must be set and HTTPSRV must be empty)
- OCSP

Microsoft Exchange integration uses a non-certified algorithm and must be disabled when in FIPS 140-2 mode.

MLPP – Limitations during a server failure

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

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.

J169 IP Phone – Minimum Software Release

The J169 IP Phone may be upgraded from SIP R1.5.0.0 to SIP R2.0.0.0 software. However, downgrade from R2.0.0.0 to 1.5.0.0 is not recommended.

J179 IP Phone – Minimum Software Release

The J179 IP Phone may be upgraded from SIP R1.5.0.0 to SIP R2.0.0.0 software. However, downgrade from R2.0.0.0 to 1.5.0.0 is not recommended.

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.

Debug mode

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

SIP_CONTROLLER_LIST

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 when interworking with Avaya Aura™. The use of Fully Qualified Domain Names (FQDN) is only supported in 3PCC environments. This applies to all sources of the SIP_CONTROLLER_LIST parameter which includes DHCP, LLDP, Web interface and the 46xxsettings.txt file

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. J100 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.

SRTP (Media Encryption)

In order to correctly use SRTP, there are various components within the network that you must correctly configure. For J100 Series IP Phones to function properly with SRTP in an Avaya Aura® environment, you must configure the equivalent parameters in Communication Manager or System Manager. Avaya strongly recommends that the following three parameters on the J100 Series IP Phones 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
```

J100 software supports 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"](http://support.avaya.com) which is available on <http://support.avaya.com> for known limitations.

Language support

The J129 IP Phones does not support a Arabic, or Chinese user interface.

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.

Headset Profiles

J100 SIP 1.5.0.0 and later software supports "Headset Profiles"² 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 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
```

SIP Transport Protocols

TCP or TLS are the recommended transport protocols. UDP transport is not supported with J100 SIP software except in a 3PCC environment.

Encryption – SHA2 and RSA 2048

J100 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 Phone (operating as the client) is able to send its Identity certificate with an enhanced digital signature (SHA2/2048 key). Additionally, this IP Phone is able to receive and validate server Identity certificates which have an enhanced digital signature (SHA2/2048 key).

Interworking – Avaya Diagnostic Server (ADS)

Avaya J100 SIP Release 2.0.0.0 supports the ADS server. 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 Diagnostic Server 3.0.3 is required to support Deskphone SIP Release 2.0.0.0 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 Phone. An IP Phone 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 Phone 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 Phone.

² J129 does not support a headset

J129/J169/J179 - Aliasing

Avaya Aura® Communication Manager 7.1 and below does not provide native support of the J129/J169/J179 IP Phones. The J129 should be administered as a "9608SIP", the J169 as a "9611SIP" or "9611SIPCC" and the J179 as a "9611SIP" or "9611SIPCC".

Until Avaya Aura® Communication Manager provides native support of the J169/J179 IP Phones, there are JBM24 feature administration limitations. To preserve existing settings for a user, feature buttons will be ported the first time they login to the phone. This allows an existing user with a 9608/9608G/9611G/9641/9641G IP Phone and BM12/SBM24 to upgrade their phone to a J169/J179 with JBM24 and preserve their BM feature buttons. Any further changes via System Manager after the initial login will not be seen until Avaya Aura® Communication Manager provides native support of the J169/J179 IP Phones and corresponding JBM24 button module.

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 IP Phone 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 IP Phone 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.

Interworking – TLS 1.2

J100 software supports TLS 1.2 and adds includes cipher suites FIPS:!ADH:!DSS:-SSLv3:DHE-RSA-AES256-SHA:AES256-SHA:DHE-RSA-AES128-SHA:AES128-SHA.



J100 software also includes a configuration parameter (TLS_VERSION) which can be used to configure the IP Phone to only use TLS 1.2. Care must be taken to only use this parameter when all components to which the IP Phone will communicate can also support TLS 1.2.

J129 - Presence

The J129 does not display presence in an Avaya Aura® network. The J129 publishes presence information for other clients that support viewing presence.

The J169 and J179 both support full presence.

VLAN separation

The J100 software supports 3 versions of VLAN separation; 1) Full VLAN separation, 2) Partial VLAN separation and 3) No VLAN separation. However, the J129 IP Phone does NOT support partial VLAN separation.

Avaya highly recommends that voice and data traffic be separated by VLANs and that voice traffic has its own VLAN.

Features not supported on the J129 Phone

The following features are not supported by the J129 IP Phone with J100 software:

- Exchange integration, WML browser, URI dialing, simultaneous display of caller name and number, redial by list, conference roster list, missed call filtering, displaying presence, Push feature, downloadable ringtones, Favorites, Personalize labels
- Bridge call appearances (except MDA)
- MLPP, Call Pickup, Hunt Group Busy, Team Button, Enhanced Call Forward, Dial Intercom, Exclusion, LNCC, Priority Calls, Whisper Page
- Interworking with Contact Center Elite (CC Elite)

Features not supported on the J169 Phone

The following features are not supported by the J169 IP Phone with J100 software:

- WML browser, simultaneous display of caller name and number, Push feature, Favorites
- WiFi

Features not supported on the J179 Phone

The following features are not supported by the J179 IP Phone with J100 software:

- WML browser, simultaneous display of caller name and number, Push feature, Favorites

Deploying the J129/J169/J179 in 3PCC Platform

The J129/J169/J179 are supported with Broadsoft Broadworks R21SP1, Zang Office R1.0 and Edgewater Network device (Edgemarc 4550). IP phone configuration file (settings file) must be deployed from a file server (HTTP or HTTPS). User backup/restore must also be deployed from a file server (HTTP or HTTPS). SIP Transport = TLS is not supported. J129 phone to work in 3PCC environment, configuration file (settings file) must have following parameter configured with value as given:

- SET ENABLE_AVAYA_ENVIRONMENT 0
- SET DISCOVER_AVAYA_ENVIRONMENT 0
- SET ENABLE_IPOFFICE 0

Provisioning of File Server Address

Phone can be provisioned using HTTP/S File Server. HTTP/S File Server address can be provided to the phone through one of the following methods:

- DHCP
- LLDP
- Device Interface

HTTPS file server has priority over the HTTP file server if both configured.

Once provisioned using one of the above methods, HTTP/S file server address can also be changed through settings file by using following parameters:

- For HTTP → HTTPSRVR, HTTPDIR, HTTPPORT
- For HTTPS → TLSSRV, TLSDIR, TLSPORT

Once File server address is changed through settings file it will override the file server address provided through DHCP or LLDP. Thus, it is advised to use this option only if different server address needs to be provided to override the DHCP.

If HTTPS file server address is configured in setting file, phone will contact to HTTPS server immediately after the download of settings file without any reboot.

Note:

Please take a note that when HTTPS file server address is configured in settings file, configure SET HTTPSRVR "" in the settings file to override the HTTPSRVR value received from DHCP. Commenting out the HTTPSRVR parameter will not override the value received from DHCP.

J100 2.0.0.0 Resolved Issues (since J100 1.1.0.1/1.5.0.0)

The following table includes issues which are resolved with this release of software compared to J100 1.1.0.1.3 and J100 1.5.0.0.15

External ID	Internal ID	Issue Description
Reboot		
	SIP96X1-22234	Intermittently phone may become stuck at restarting screen after manual clear or reboot Recovery Path: Plugging out the cable and plug-in again
1-13521836532	SIP96X1-30247	J129 crash when it updates config with higher RTP_PORT_LOW
1-12612504521	SIP96X1-23404	Phone reboots when connecting to large AAC conf calls
IP Office		
1-13365980662	SIP96X1-29279	Upon simultaneous restart of primary & connected IP400v2 expansion, J129 phones are unable to failover and automatically log back in
User Interface		
	SIP96X1-23878	J129 - "Emerg" softkey is displayed on "Idle logged out" screen when SIP_CONTROLLER_LIST is empty and PHNEMERGNUM is not configured
	SIP96X1-25251	J169/J179 - Deskphone incorrectly shows a very large value for packet loss in the case of only incoming RTP (eg. Music on hold) and low packet loss.
	SIP96X1-22458	J129 - User does not receive forced log out message while the phone they are registered to is in a locked state and the user is active in the Admin Menu
Networking		
	SIP96X1-25446	J129 phone displays "Authentication failed" in response to a successful 802.1X response from the switch when the switch is set to Auto. Work around is to set the switch to "Forced Authorized".
	SIP96X1-25428	J129 phone displays "Authentication failed" forever after resetting to default from the Admin menu. Work around is to reboot the phone again.
	SIP96X1-21088	J129 - Phone does not display 802.1X Authentication failed screen after receiving EAP-Failure frame from switch
1-12606934290	SIP96X1-23450	Phone unable to connect to Office365 Exchange Cloud Server Refer to EXCHANGE_AUTH_USERNAME_FORMAT parameter.
Configuration		
	SIP96X1-23102	J129 - AUDASYS parameter is not supported
MLPP		

External ID	Internal ID	Issue Description
	SIP96X1-24689	J169/J179 - Make precedence call Flash level from phone A to phone B, release the call. On phone A, press "Priority" soft key then select Flash level. Press CA 1 on phone A, then press "Redial" soft key, the call is made as normal call, not precedence call.

Unresolved issues in J100 2.0.0.0.45

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
Avaya Aura®		
1-12671341066	SIP96X1-24119	ELD Rules not working. User is not able to dial 11 digit national calls from history.
	SIP96X1-23746	Deskphone accesses Avaya Equinox™ 9.0 conference bridge and logs in as moderator. User uses the "Add" softkey to add another user to the conference bridge. If the user goes into Network Information -> Audio Parameters, the display shows "No Call".
	SIP96X1-17977	Configuration file includes SET ENABLE_G729 2. User A and User B are in call. Then on User B, press "Transfer" softkey and dial to User C. During User B and User C are in call, User A holds its call. At that time, User B completes his transfer call to User C by pressing "Complete" softkey. The call is transferred successfully. When User A unholds the call, there is no speechpath.
	SIP96X1-20240	Phone B is configured with EC500 feature with cell phone number. Make call from phone A to phone B and answer the call on Cell phone. Press bridge soft key on phone B, then from phone B make unattended transfer to phone C. Answer the call on C -> No voice speech path between phone A and C.
	SIP96X1-15791	Phone A has failed over to IP Office due to inability to reach configured Session Managers. User adds a new contact and tracks presence. Following recovery, the presence of the contact is shown as "unknown". <i>Workaround: Log out and then back in.</i>
	SIP96X1-11378	System is configured for SBC High Availability. Two remote phones are in an active call. The primary SBC restarts. Immediately after the restart is completed, the secondary SBC also restarts. The phones will lose their audio path and reboot.
	SIP96X1-23977	Deskphone is configured for FIPS mode and has a valid identity certificate. If an attempt is made to install a new certificate which is not FIPS-compliant, then the Deskphone does not display a "certificate rejected" message but does continue to use the original valid certificate.
	SIP96X1-23938	J129 Phone doesn't display "Non-AST/Fail-Over" icon after failover to non-AST environment when you are not on the idle screen and failover happens.

External ID	Internal ID	Issue Description
	SIP96X1-23936	After entering Login credentials, sometimes there is no button effect for 8-10 seconds on J129. It is observed once any other user logouts having 250 contacts and immediately other user tries to login.
	SIP96X1-23905	J129 phone does not play ringing tone for second call when active call is emergency call
	SIP96X1-23883	J129 - Phone does not generate call log of Emergency call in Locked state when Emergency number was added in Contacts
	SIP96X1-23863	J129 - Phone does not always update sip proxies list after changing order of sip proxies in SMGR
	SIP96X1-23238	J129 - Phone displays conference icon and softkeys after other MDA user deactivates call-park feature
	SIP96X1-22458	J129 - User does not receive forced log out message while the phone they are registered to is in a locked state and the user is active in the Admin Menu
	SIP96X1-20779	J129 - Phone does not enable call-park feature when the feature is activated from another MDA user
	SIP96X1-20316	J129 - Server field ID display does not index to the right after clearing 8 characters
	SIP96X1-26755	J129 - Local call forward does not appear on Feature screen for using after failover to Audiocodes
	SIP96X1-28106	Phone does not display NewCall SK for making the second calls after completing failover to BSM in active call
	SIP96X1-28107	J129 phone can't make Single Step Transfer usingTSAPI
	SIP96X1-28113	Guest Login: History LED keeps on lit, on primary user even after guest login logs out
	SIP96X1-28155	J129-Intermittent- 802.1X authentication failure text mixed up with admin menu text when phone is in admin menu.
	SIP96X1-28284	Navigation does not work for the first pressing in "EAP-MD5 Authentication failed" screen
	SIP96X1-28651	Unexpected Softkeys after Cancel consult with 3rd party
	SIP96X1-29616	SIP proxy server does not switch to IPv4 when invalid Phone(V6) is set in WebUI
	SIP96X1-29823	J179 phone does not display added contact during limbo state
	SIP96X1-29855	Intermittent - Phone is stuck at PKCS12 installation screen during boot up in Wifi mode
	SIP96X1-29926	J129- One way speech path after holding/resuming the call with codec OPUS-WB20k and media encryption 3-srtp-aescm128-hmac80-unauth.
	SIP96X1-29927	Phone initiates call to voice mail on 2nd CA
	SIP96X1-30159	J179/J169 - App in Customize key is not translated to new language, which is different from English
	SIP96X1-30214	Characters of features on JBM24 are Bold and do not display clearly in Thai language

External ID	Internal ID	Issue Description
	SIP96X1-30262	Remote Control icon is not getting displayed for logged out J169 phones
	SIP96X1-30510	[Web] Web displays SIP User ID and Authentication User ID inconsistently after Guest User is logged out.
	SIP96X1-31097	Parameter PKCS12_PASSWD_RETRY works incorrectly.
	SIP96X1-31177	J100 phones take time to perform 'hold/transfer' SK operation if these SKs are pressed after recording an active call.
	SIP96X1-31276	Phone displays "No match found" when searching contact which created with only Last name on Exchange Server
	SIP96X1-31356	Oneway speech path after fake hold and resume (failover)
	SIP96X1-31369	J129/J169/J179 - No voice speech path after hold both phones and resume the call (SRTP call)
	SIP96X1-31597	Seen twice - J129 phone reboots and generates coredump tContactManager when use extension with 250 contacts
IP Office		
	SIP96X1-23804	J129 contacts with IP Office: Sometimes 'New' softkey is displayed after adding 250 contacts.
	SIP96X1-31066	J179 - Headset call - make hold/unhold call goes to handsfree on speaker
CCElite		
	SIP96X1-30907	[CCElite] - Phone does not display Call Timer in half width mode
	SIP96X1-29794	[CCElite] Call transfer - Phone does not display collect digit
	SIP96X1-29804	CCElite] Call transfer- Agent does not send the Avaya-User-Data and UI-Info data in the INVITE
3PCC		
	SIP96X1-23559	J129 - User_Store - Phone is not making PUT request after receiving 404 in response of a GET query after adding first contact if HTTP Authentication is enabled in server and Authentication is ignored by user when it prompts. <i>Workaround: Edit contact again and perform Manual Backup</i>
	SIP96X1-23211	J129 - Glare handling for retransmitted INVITE and 407 with different nonce <i>Workaround: Change Timer T1</i>
	SIP96X1-23183	J129 - User_Store - If user changed a parameter that triggered a Backup. If the backup is in progress and the user logs out and new user is logging immediately may have their "restore" impacted and it may not work.
	SIP96X1-21314	J129 - Phone does not allow contacts to be added as speed dial entries until PPM update is complete

External ID	Internal ID	Issue Description
All Platforms		
	SIP96X1-23890	J129 - "@" character is not supported for User ID, Contacts. If "@" character is configured, phone will ignore all the characters after "@" including "@" character. For CLI display, phone will not display name or number after "@" including "@" character.
	SIP96X1-23850	J129 - When downgrade fails, Upgrade info screen is blank
	SIP96X1-23791	J129 - 802.1x – Phone is not displaying 802.1x credential screen if phone receives EAP-Failure packet. This case happens only if credentials are changed in Radius Server during working environment. Workaround: Reboot the phone
	SIP96X1-22231	J129 - MIB browser displays value of "endptLANGINUSE" incorrectly
	SIP96X1-20743	J129 - Phone reboots a second time after the user comments out the proxy address in settings file.
	SIP96X1-20372	J129 - Phone does not display SCEP notifications while it is downloading identity certificate from CA server
	SIP96X1-29549	The backlight for JBM24 is turned on when phone is locked
	SIP96X1-29607	[DES] Auto Config prompt is not displayed if DES is manually invoked from Admin Menu
	SIP96X1-30248	transducer unexpectedly switches to Headset!
	SIP96X1-30718	Phone display message "Contact already exists" when edit ringtone
	SIP96X1-30715	Phone display "Feature not available" while customizing line keys
	SIP96X1-30771	J129 - Cannot back to provisioning screen 1 after enter to provisioning screen 2
	SIP96X1-30908	Web UI - Need to clarify item Old Web Admin Password in Phone Admin Password menu
	SIP96X1-30948	Phone displays number of BCA incorrectly after moving in customize key.
	SIP96X1-31033	Quick search appear and show empty after logout/login
	SIP96X1-31080	Pressing key "0" for the first input in contact group name then press other key, other key is doubled

Appendix 1 – Supported Hardware

J100 SIP 2.0.0.0 software is supported on the following models of IP Phones. Models may ship from the factory with a different load of software pre-installed. As such, they should be upgraded to this release on first installation.

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
700512392	J129 IP PHONE	J129D01A	
700513638	J129 IP PHONE NO PWR SUPP	J129D01A	
700512969	J129 IP PHONE 3PCC W/O PWR SUPP	J129D01A	
700513639	J129 IP PHONE 3PCC W/CERT	J129D01A	
700512393	J129 IP PHONE GSA	J129D01A	
700513634	J169 IP PHONE NO PWR SUPP	J169D01A	Must use J100 1.5 or later software.
700513635	J169 IP PHONE GSA	J169D01A	Must use J100 1.5 or later software.
700513636	J169 IP PHONE 3PCC	J169D01A	Must use J100 1.5 or later software.
700513569	J179 IP PHONE NO PWR SUPP	J179D02A	Must use J100 1.5 or later software.
700513629	J179 IP PHONE GSA	J179D02A	Must use J100 1.5 or later software.
700513630	J179 IP PHONE 3PCC	J179D02A	Must use J100 1.5 or later software.

Appendix 2 – Release History

The following table provides a history of the J100 SIP software releases. The “ID” column shows the identifier of this software which is seen in the “About” menu item.

Release	ID	Date	Link to Readme file
1.0.0.0	1.0.0.0.43	Dec 2016	https://support.avaya.com/css/P8/documents/101033485
1.1.0.0	1.0.0.0.15	Mar 2017	https://support.avaya.com/css/P8/documents/101037079
1.1.0.1	1.0.0.1.3	Aug 2017	https://support.avaya.com/css/P8/documents/101042514
1.5.0.0	1.5.0.0.15	Mar 2018	http://support.avaya.com/css/P8/documents/101047039
2.0.0.0	2.0.0.0.45	April 2018	https://support.avaya.com/css/P8/documents/101048016

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=P1661

New parameters.

```
##### LOGIN SETTINGS #####
##

##
## SHOW_LAST_EXTENSION specifies whether extension is presented after logout.
## Value Operation
## 0 Extension is not presented after logout (Default)
## 1 Extension is presented after logout
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later
## SET SHOW_LAST_EXTENSION 1

#####
##
## WI-FI SETTINGS
##
#####
##
##### NETWORK MODE OF OPERATION #####
##
## WIFISTAT specifies whether the user is given an option to enable Wi-Fi.
## Value Operation
## 0 Wi-Fi is disabled and the user is not given an option to enable it; the phone will only use the Ethernet interface.
## 1 The user is given an option to enable Wi-Fi; the phone will connect to Ethernet (Default), unless the UI is used to manually switch to Wi-Fi.
## 2 Wi-Fi is the preferred interface, but manual override to a different SSID or to Ethernet is allowed; the phone will connect to WLAN_ESSID (i.e., the pre-configured Wi-Fi network) unless the phone UI is used to manually switch to another SSID or to Ethernet. Associated pre-configured Wi-Fi network security parameters must also be specified.
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later; values 0-2 are supported.
## Only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT). If the phone does not support Wi-Fi/BT, WIFISTAT will be internally set to 0, regardless of the value received from 46xxsettings.txt.
## The Administrator should always test a new settings file configuration on a single phone before committing it to several phones, as a configuration error (such as specifying an incorrect WLAN_ESSID or Wi-Fi security settings) will cause phones to become disconnected from the network, necessitating manual correction on each phone's local User Interface, as the phone will not be reachable via any other means.
## If the phone is using the pre-configured network (i.e., Ethernet or a specific Wi-Fi WLAN_ESSID), and then the phone UI is used to manually switch to a different network, the phone will enter Manual Network Configuration Mode, which will cause the phone to continue to connect to the manually-configured network on subsequent reboots, regardless of the pre-configured network specified by WIFISTAT and any associated parameters.
## There are 2 ways to return the phone to Automatic Network Configuration mode (i.e., to comply again with WIFISTAT, and if WIFISTAT=2, also WLAN_ESSID and associated pre-configured Wi-Fi network security parameters):
## - Use the phone's UI to explicitly toggle "Network config" from "Manual" to "Auto".
## - Change WIFISTAT to 0 and reboot the phone, which will force the phone to use Ethernet, after which, WIFISTAT can be changed to the desired value and the phone rebooted again.
## Avaya Vantage Devices SIP R1.0.0.0 and later; values 0-1 are supported.
## H1xx SIP R1.0 and later; values 0-1 are supported.
## SET WIFISTAT 0
##
```



```

## WIFIAPSTAT specifies whether the user is given an option to enable Wi-Fi hotspot.
## Value Operation
## 0 Wi-Fi hotspot is disabled and the user is not given an option to enable it (default)
## 1 The user is given an option to enable Wi-Fi hotspot
## This parameter is supported by:
## Avaya Vantage Devices SIP R1.0.0.0 and later
## SET WIFIAPSTAT 1
##
## WIFI_CON_STATUS_ON_LOGOUT specifies whether ALL wireless connections will be forgotten (including static networks) when the
device is logout.
## Value Operation
## 0 ALL Wi-Fi connections are forgotten (including static networks and all authentication options (802.1x, WEP/WPA)) when the
device moves to logout state
## 1 ALL Wi-Fi connections are preserved when the device moves to logout state (and in particular, the active Wi-Fi connection
remains as it is)(default)
## Note: when WIFI_CON_STATUS_ON_LOGOUT is set to 1, then the Wi-Fi credentials are shared across all users. When
WIFI_CON_STATUS_ON_LOGOUT is set to 0 (and the network mode is Wi-Fi),
## after each logout, then the new/same user is required to enter Wi-Fi credentials before being able to login. When there is no Wi-Fi
connectivity, emergency calls cannot be established.
## This parameter is supported by:
## Avaya Vantage Devices SIP R1.0.0.0 and later; not applicable when Avaya Vantage Open application is used.
## SET WIFI_CON_STATUS_ON_LOGOUT 0
##
##### NETWORK CONFIGURATION USER PRIVILEGE #####
##
## ENABLE_NETWORK_CONFIG_BY_USER specifies whether network configuration can be modified by the end user, either via the
Settings menu, or when there is a network issue that
## could be remedied by the user.
## Value Operation
## 0 Disabled
## 1 Enabled (Default)
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET ENABLE_NETWORK_CONFIG_BY_USER 0
##
##### WI-FI REGULATORY DOMAIN SETTINGS #####
##
## WLAN_COUNTRY specifies the 2-character ISO 3166 Alpha-2 Country code representing the Wi-Fi regulatory domain.
## The default value is "US".
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WLAN_COUNTRY CA
##
## WLAN_ENABLE_80211D specifies whether 802.11d is used or not. When enabled, the Wi-Fi regulatory domain will be used
according to the 802.11d Country IE provided by the
## connected Wi-Fi Access Point. When disabled, the Wi-Fi regulatory domain will be used according to WLAN_COUNTRY.
## Note: The use of 802.11d is banned in the United States, so this parameter must NOT be set to 1 in this regulatory domain.
## Value Operation
## 0 Disabled (Default)
## 1 Enabled
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WLAN_ENABLE_80211D 1
##
##### PRE-CONFIGURED WI-FI NETWORK #####
##
## WLAN_ESSID specifies the SSID string of the pre-configured Wi-Fi network.
## The value can contain 1 to 32 characters; the default value is null ("").
## Valid characters are:
## A-Z, a-z, 0-9, and the following: *.-!$%&'[]+,:;/\=@~#
## The space character, ASCII 0x20, is NOT supported.
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WLAN_ESSID mywlanSSID
##
## WLAN_SECURITY specifies the pre-configured Wi-Fi network Security Method.
## Value Operation
## none No security (Default)

```

```

## wep WEP security
## wpa2psk WPA/WPA2 PSK (pre-shared key) security
## wpa2e WPA2 Enterprise security (802.1x authentication)
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WLAN_SECURITY wpa2e
##
##### Pre-configured Wi-Fi network WEP security settings #####
##
## WEP_DEFAULT_KEY specifies the pre-configured Wi-Fi network index of the WEP default key.
## This parameter is only applicable when WIFISTAT enables Wi-Fi and WLAN_SECURITY is wep.
## The range of valid values is 1-4; the default value is 1.
## Only Shared Key authentication is supported. Open authentication is NOT supported.
## Some Wi-Fi Routers can only be configured with 1 WEP key, in which case ONLY WEP_KEY1 should be set.
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WEP_DEFAULT_KEY 2
##
## WEP_KEY_LEN specifies the pre-configured Wi-Fi network WEP key length.
## This parameter is only applicable when WIFISTAT enables Wi-Fi and WLAN_SECURITY is wep.
## Value Operation
## 64bit WEP keys of 64 bits
## 128bit WEP keys of 128 bits (default)
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WEP_KEY_LEN 64bit
##
## WEP_KEY1/2/3/4 specifies the pre-configured Wi-Fi network WEP Keys 1 to 4.
## These parameters are only applicable when WIFISTAT enables Wi-Fi and WLAN_SECURITY is wep.
## The value can contain 10 (for 64-bit WEP) or 26 (for 128-bit WEP) ASCII-Hex digits; the default value is null ("").
## Valid characters are:
## 0-9, A-F
## These parameters are supported by:
## J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WEP_KEY1 0123456789ABCDEF0123456789
## SET WEP_KEY2 123456789ABCDEF01234567890
## SET WEP_KEY3 23456789ABCDEF012345678901
## SET WEP_KEY4 3456789ABCDEF0123456789012
##
##### Pre-configured Wi-Fi network WPA/WPA2 PSK or 802.1X EAP security settings #####
##
## WLAN_PASSWORD specifies the pre-configured Wi-Fi network password.
## This parameter is only applicable when WIFISTAT enables Wi-Fi and:
## - WLAN_SECURITY is wpa2psk
## or
## - WLAN_SECURITY is wpa2e and WLAN_WPA2E_EAP_METHOD is PEAP and WLAN_WPA2E_EAP_PHASE2 is MSCHAPV2
## If WLAN_SECURITY is wpa2psk, the value can contain 8 to 63 characters.
## If WLAN_SECURITY is wpa2e, the value can contain 1 to 32 characters.
## The default value is null ("").
## Valid characters are:
## A-Z, a-z, 0-9, and the following: *.-!$%&'()+:;./\=@~#
## The space character, ASCII 0x20, is NOT supported.
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WLAN_PASSWORD Avaya123
##
## WLAN_WPA2E_EAP_METHOD specifies the pre-configured Wi-Fi network 802.1x EAP method.
## This parameter is only applicable when WIFISTAT enables Wi-Fi and WLAN_SECURITY is wpa2e.
## Value Operation
## PEAP Connect using PEAP (Default)
## TLS Connect using TLS
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WLAN_WPA2E_EAP_METHOD TLS
##
## WLAN_WPA2E_EAP_PHASE2 is the pre-configured Wi-Fi network 802.1x phase 2 Method.
## This parameter is only applicable when WIFISTAT enables Wi-Fi and WLAN_SECURITY is wpa2e and WLAN_WPA2E_EAP_METHOD
is PEAP.

```

```

## Value    Operation
## none     No phase 2 authentication (Default, but not currently supported)
## MSCHAPV2 As of J100 2.0, MUST be set to this value for forward compatibility
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WLAN_WPA2E_EAP_PHASE2 MSCHAPV2
##
## WLAN_WPA2E_IDENTITY specifies the pre-configured Wi-Fi network 802.1x identity.
## This parameter is only applicable when WIFISTAT enables Wi-Fi and WLAN_SECURITY is wpa2e and:
##   - WLAN_WPA2E_EAP_METHOD is PEAP and WLAN_WPA2E_EAP_PHASE2 is MSCHAPV2
##   or
##   - WLAN_WPA2E_EAP_METHOD is TLS
## The value can contain 1 to 32 characters; the default value is null ("").
## Valid characters are:
##   A-Z, a-z, 0-9, and the following: *.-!$%&'() +,;:/\=@~#
## The space character, ASCII 0x20, is NOT supported.
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WLAN_WPA2E_IDENTITY User123
##
## WLAN_WPA2E_ANONYMOUS_IDENTITY specifies the pre-configured Wi-Fi network 802.1x anonymous identity.
## This parameter is only applicable when WIFISTAT enables Wi-Fi and WLAN_SECURITY is wpa2e and
##   WLAN_WPA2E_EAP_METHOD is PEAP and WLAN_WPA2E_EAP_PHASE2 is MSCHAPV2.
## The value can contain 1 to 32 characters; the default value is null ("").
## Valid characters are:
##   A-Z, a-z, 0-9, and the following: *.-!$%&'() +,;:/\=@~#
## The space character, ASCII 0x20, is NOT supported.
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WLAN_WPA2E_ANONYMOUS_IDENTITY foo@example
##
##### WLAN LAYER 2 QOS SETTINGS #####
##
## WLAN_L2QUAD specifies the layer 2 priority value for audio frames generated by the telephone when Wi-Fi interface is used.
## Valid values are 0 through 7; the default value is 6.
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WLAN_L2QUAD 1
##
## WLAN_L2QSIG specifies the layer 2 priority value for signaling frames generated by the telephone when Wi-Fi interface is used.
## Valid values are 0 through 7; the default value is 3.
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WLAN_L2QSIG 1
##
##### WLAN LAYER 3 QOS SETTINGS #####
##
## WLAN_DSCPAUD specifies the layer 3 Differentiated Services (DiffServ) Code Point for audio frames generated by the telephone when
Wi-Fi interface is used.
## Valid values are 0 through 63; the default value is 46.
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WLAN_DSCPAUD 1
##
## WLAN_DSCPSIG specifies the layer 3 Differentiated Services (DiffServ) Code Point for signaling frames generated by the telephone
when Wi-Fi interface is used.
## Valid values are 0 through 63; the default value is 34.
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later; only J129 and J179 support a pluggable Wi-Fi/BT module (J169 does not support Wi-Fi/BT)
## SET WLAN_DSCPSIG 1
##

##### HTTP/S WEB SERVER #####
##
## ENABLE_WEBSERVER specifies whether the HTTP/S WEB Server is enabled or disabled.
## Value Operation
## 0 Disabled (default)
## 1 Enabled

```

```

## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later; If the phone boots up in 3PCC environment and ENABLE_WEBSERVER is not explicitly set 0, it will be
internally set to 1.
##           This is to enable web server by default in 3PCC environments.
## SET ENABLE_WEBSERVER 1
##
## WEBSERVER_ON_HTTP specifies whether HTTP access to the Web Interface is enabled or disabled.
## The WEB Server will be accessible using HTTP as long ENABLE_WEBSERVER and WEBSERVER_ON_HTTP are set to 1.
## The WEB Server will be accessible using HTTPS as long ENABLE_WEBSERVER is set to 1 AND (Identity certificate is installed in
factory or
## using WEB/SCEP/PKCS12 file download).
## Value Operation
##   0   Web Server will not be accessible via HTTP
##   1   Web Server will be accessible via HTTP (Default)
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later
## SET WEBSERVER_ON_HTTP 0
##
## WEB_HTTP_PORT specifies the HTTP port on which the Web Server running on the phone will be accessed using HTTP.
## Valid values are 80-65535. The default value is 80.
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later
## SET WEB_HTTP_PORT 81
##
## WEB_HTTPS_PORT specifies the HTTPS port on which the Web Server running on the phone will be accessed using HTTPS.
## Valid values are 443-65535. The default value is 443.
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later
## SET WEB_HTTPS_PORT 444
##
## FORCE_WEB_ADMIN_PASSWORD specifies the password to access the phone through Web as Administrator.
## From settings file, FORCE_WEB_ADMIN_PASSWORD will be used instead of WEB_ADMIN_PASSWORD (configured from the Web
Interface).
## As long as FORCE_WEB_ADMIN_PASSWORD is configured in the Settings file, it will be used as the Web admin password.
## It will overwrite any password user might have configured from the Web Interface.
## Valid values are: 8 to 31 alphanumeric characters including upper, lower and special characters.
## Special characters allowed:~!@#%&*_-=~\|{}[];';<>.,?/. The default is "27238".
## Note: WEB_ADMIN_PASSWORD has no interaction with PROCPSWD or ADMIN_PASSWORD.
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later
## SET FORCE_WEB_ADMIN_PASSWORD HelloWorld!01

##### IDLE TIMER SETTINGS #####
##

## SCREENSAVER_IMAGE specifies a list of screensaver images. The default value is "".
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later (J169 and J179 only)
##           Up to 5 background images are supported. Only jpeg/jpg files are supported.
##           The maximum size of any jpeg file is 256 KB. The filenames are case insensitive.
##           J169/J179 screen resolution is 320 pixels x 240 pixels. J179 color depth is 16 bits.
##           J129 screen resolution is 128 pixels x 32 pixels.
##           The files shall be stored in the same directory defined by HTTPDIR / TLSDIR.
## SET SCREENSAVER_IMAGE "screensaver_example1.jpg,screensaver_example2.jpeg"
##
## SCREENSAVER_IMAGE_DISPLAY specifies the administrator choice of screensaver image.
## The filename shall be one of the filenames listed in SCREENSAVER_IMAGE.
## If SCREENSAVER_IMAGE_SELECTABLE is set to 1 then the end user may override this setting.
## The default value is "".
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later (J169 and J179 only)
## SET SCREENSAVER_IMAGE_DISPLAY screensaver_example1.jpg
##
## SCREENSAVER_IMAGE_SELECTABLE specifies whether end users are allowed to choose screensaver images
## (and overrides administrator choice as configured using SCREENSAVER_IMAGE_DISPLAY parameter).
## Value Operation
##   0   End user is not allowed to choose screensaver image and will not see the screensaver image selection in the Settings -> Display
menu.

```

```

## 1 End user is allowed to choose the screensaver image from the Settings -> Display menu (Default)
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later (J169 and J179 only)
## SET SCREENSAVER_IMAGE_SELECTABLE 0
##
## BACKLIGHT_SELECTABLE specifies whether backlight timer will be determined per administrator (BAKLIGHTOFF) or user
configuration.
## Value Operation
## 0 "Backlight timer" value (BAKLIGHTOFF) will be obtained from 46xxsettings.
## 1 "Backlight timer" value (BAKLIGHTOFF) can be set by user using "User Menu->Settings->Display" submenu (Default)
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later (J169 and J179 only)
## SET BACKLIGHT_SELECTABLE 0

##### OTHER SIP-ONLY SETTINGS #####
##

##
## SOFTKEY_CONFIGURATION specifies which feature will show up on which softkey on the J129 phone screen. Does not apply to other
J100 models.
## The features are defined as follows:
## 0 = Redial
## 1 = Contacts
## 2 = Emergency
## 3 = Recents
## 4 = Voicemail
## The default is "0,1,2". i.e. default softkeys are Redial, Contacts, Emerg.
## Note: RULES:
## If a value is not presented then the softkey is blank
## e.g. SOFTKEY_CONFIGURATION 0,,2 => Redial, Blank, Emerg
## If a value is outside the range then the softkey is blank
## e.g. SOFTKEY_CONFIGURATION 0,1,7 => Redial,Contacts, Blank
## e.g. SOFTKEY_CONFIGURATION 0,&GGI^,2 => Redial, Blank, Emerg
## If there are not enough values in the range then the remaining softkeys will be blank
## e.g. SOFTKEY_CONFIGURATION 4,3 = Voicemail,Recents, Blank
## ADDITIONAL NOTES: Even if PHNEMERGNUM is defined the EMERG softkey must be defined.
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later (J129 only)
## SET SOFTKEY_CONFIGURATION 1,2,3

##### DISPLAY SETTINGS #####
##

##
## BACKGROUND_IMAGE specifies a list of background images. The default value is "".
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later (J169 and J179 only)
## Up to 5 background images are supported. Only jpeg/jpg files are supported.
## The maximum size of any jpeg file is 256 KB. The filenames are case insensitive.
## J169/J179 screen resolution is 320 pixels x 240 pixels. J179 color depth is 16 bits.
## J129 screen resolution is 128 pixels x 32 pixels.
## The files shall be stored in the same directory defined by HTTPDIR / TLSDIR.
## SET BACKGROUND_IMAGE "background_example1.jpg,background_example2.jpeg"
##
## BACKGROUND_IMAGE_DISPLAY specifies the administrator choice of background image.
## The filename shall be one of the filenames listed in BACKGROUND_IMAGE.
## If BACKGROUND_IMAGE_SELECTABLE is set to 1 then the end user may override this setting.
## The default value is "".
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later (J169 and J179 only)
## SET BACKGROUND_IMAGE_DISPLAY background_example1.jpg
##
## BACKGROUND_IMAGE_SELECTABLE specifies whether end users are allowed to choose background images
## (and overrides administrator choice as configured using BACKGROUND_IMAGE_DISPLAY parameter).
## Value Operation
## 0 End user is not allowed to choose background image and will not see the background image selection in the Settings -> Display
menu.
## 1 End user is allowed to choose the background image from the Settings -> Display menu (Default)

```

```
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later (J169 and J179 only)
## SET BACKGROUND_IMAGE_SELECTABLE 0
```

Changed parameters.

```
##### LAYER 2 VLAN AND QOS SETTINGS #####
##
## L2Q specifies whether layer 2 frames generated by the telephone will have IEEE 802.1Q tags.
## Value Operation
## 0 Auto - frames will be tagged if the value of L2QVLAN is non-zero (default).
## 1 On - frames will always be tagged.
## 2 Off - frames will never be tagged.
## Note: This parameter may also be set via DHCP or LLDP.
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later - if L2QVLAN == 0, L2Q is treated as 2 (disabled).
##   Avaya Vantage Devices SIP R1.0.0.0 and later. Note: Value 1 has the same behavior as value 0.
##   J169/J179 SIP R1.5.0 - if L2QVLAN == 0, L2Q is treated as 2 (disabled).
##   J129 SIP R1.0.0.0 and later
##   H1xx SIP R1.0 and later. Note: Value 1 has the same behavior as value 0.
##   96x1 H.323 R6.0 and later
##   96x1 SIP R6.0 and later; R7.1.0.0 and later, if L2QVLAN == 0, L2Q is treated as 2 (disabled).
##   B189 H.323 R1.0 and later
##   96x0 H.323 R1.0 and later
##   96x0 SIP R1.0 and later
## SET L2Q 0
##
## L2QVLAN specifies the voice VLAN ID to be used by IP telephones.
## Valid values are 0 through 4094; the default value is 0.
## Note: This parameter may also be set via DHCP or LLDP.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   Avaya Vantage Devices SIP R1.0.0.0 and later
##   H1xx SIP R1.0 and later
##   96x1 H.323 R6.0 and later
##   96x1 SIP R6.0 and later
##   B189 H.323 R1.0 and later
##   96x0 H.323 R1.0 and later
##   96x0 SIP R1.0 and later
## SET L2QVLAN 5
##
## L2QAUD specifies the layer 2 priority value for audio frames generated by the telephone.
## Valid values are 0 through 7; the default value is 6.
## Note: This parameter may also be set via LLDP and H.323 signaling,
##   which would overwrite any value set in this file.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   H1xx SIP R1.0 and later
##   96x1 H.323 R6.0 and later
##   96x1 SIP R6.0 and later
##   B189 H.323 R1.0 and later
##   96x0 H.323 R1.0 and later
##   96x0 SIP R1.0 and later
## SET L2QAUD 7
##
## L2QSIG specifies the layer 2 priority value for signaling frames generated by the telephone.
## Valid values are 0 through 7; the default value is 6.
## Note: This parameter may also be set via LLDP or H.323 signaling,
##   which would overwrite any value set in this file.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   H1xx SIP R1.0 and later
##   96x1 H.323 R6.0 and later
##   96x1 SIP R6.0 and later
##   B189 H.323 R1.0 and later
```

```

## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## SET L2QSIG 7
##
## VLANSEP specifies whether VLAN separation will be enabled by the built-in Ethernet switch
## while the telephone is tagging frames with a non-zero VLAN ID. When VLAN separation is enabled,
## only frames with a VLAN ID that is the same as the VLAN ID being used by the telephone
## (as well as priority-tagged and untagged frames) will be forwarded to the telephone.
## Also, if the value of PHY2VLAN (see below) is non-zero, only frames with a VLAN ID that is
## the same as the value of PHY2VLAN (as well as priority-tagged and untagged frames) will be
## forwarded to the secondary (PHY2) Ethernet interface, and tagged frames received on the
## secondary Ethernet interface will have their VLAN ID changed to the value of PHY2VLAN and
## their priority value changed to the value of PHY2PRIO (see below).
## Value Operation
## 0 Disabled.
## 1 Enabled if L2Q, L2QVLAN and PHY2VLAN are set appropriately (default).
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169, J179 only)
## Avaya Vantage Devices SIP R1.1.0.0 and later for K165/K175 models with embedded Ethernet switch; see comments for H1xx
SIP R1.0 and later.
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## H1xx SIP R1.0 and later; VLAN separation supported on H1xx have the following exceptions:
## 1. Priority-tagged and untagged frames from the network port will be forwarded to the PC port only when VLANSEP==1,
## H1xx sends tagged packets (L2Q==0 or 1 and VLANTEST==0 or timer < VLANTEST) and L2QVLAN<>0, else to both phone
and PC ports.
## 2. No enforcement of PHY2VLAN and PHY2PRIO on tagged VLAN packets received from PC port. If VLANSEP==1,
## H1xx sends tagged packets (L2Q==0 or 1 and VLANTEST==0 or timer < VLANTEST) and 0<>PHY2VLAN<>L2QVLAN<>0
then:
## a. Untagged packets from PC port will be tagged with PHY2VLAN and priority==0.
## b. Tagged packets will be forwarded as tagged packets only if their VLAN equal to PHY2VLAN.
## Otherwise the packets from PC will be sent unmodified.
## Only in case of VLANSEP==1, H1xx sends tagged packets (L2Q==0 or 1 and VLANTEST==0 or timer < VLANTEST) and
0<>PHY2VLAN<>L2QVLAN<>0,
## there will be full separation between PC and phone traffic. In all other cases, PC traffic can reach the phone.
## 3. When VLANSEP ==0, H1xx sends untagged packets even if L2Q==0 or 1 and VLANTEST==0 or timer < VLANTEST.
## SET VLANSEP 0
##
## VLANSEPMODE specifies whether full VLAN separation will be enabled by the built-in Ethernet switch
## while the telephone is tagging frames with a non-zero VLAN ID. This VLAN separation is enabled when:
## VLANSEP=1, L2QVLAN<> PHY2VLAN (and both has value different than 0), L2Q is auto (0) or (1) tagging.
## In this new VLAN separation scheme:
## - Untagged packets from PC port will be forwarded to network port only as untagged packets.
## - Tagged packets from PC port will be forwarded to network port only as tagged packets only in case
## their VLAN is equal to PHY2VLAN.
## In this mode, tagged and untagged packets from PC port will never reach phone's port.
## - 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, then the VLAN separation is based on previous releases where untagged packets
## from PC port can reach the phone.
## Please note that PHY2PRIO is NOT supported when VLANSEPMODE is 1.
## Value Operation
## 0 Disabled
## 1 Enabled
## This parameter is supported by:
## J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later (J169/J179 only), Default is 0.
## 96x1 SIP R7.1.0.0 and later, Default is 0.
## 96x1 H.323 R6.6 and later, Default is 0.
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later (J129 only); Default is 1. VLANSEP is not supported by J129. The
conditions for VLAN separation mode are
## as described above (except no support for VLANSEP). If one the conditions is not fulfilled then J129
## will get any tagged/untagged unknown/broadcast/multicast/known DA equal to CPU MAC address packets from the network
or PC port.
## SET VLANSEPMODE 1

```



```

##
## PHY2VLAN specifies the VLAN ID to be used by frames forwarded to and from the secondary
## (PHY2) Ethernet interface when VLAN separation (see VLANSEP above) is enabled.
## Valid values are 0 through 4094; the default value is 0.
## Note: This parameter may also be set via LLDP.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later
##   Avaya Vantage Devices SIP R1.1.0.0 and later for K165/K175 models with embedded Ethernet switch
##   H1xx SIP R1.0 and later
##   96x1 H.323 R6.0 and later
##   96x1 SIP R6.0 and later
##   96x0 H.323 R1.0 and later
##   96x0 SIP R1.0 and later
## SET PHY2VLAN 1
##
## PHY2PRIO specifies the layer 2 priority value to be used for frames received on the secondary
## (PHY2) Ethernet interface when VLAN separation (see VLANSEP above) is enabled.
## Valid values are 0 through 7; the default value is 0.
## The parameter is not supported when VLANSEPMODE is 1.
## This parameter is supported by:
##   J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
##   96x1 H.323 R6.0 and later
##   96x1 SIP R6.0 and later
##   96x0 H.323 R1.0 and later
##   96x0 SIP R1.0 and later
## SET PHY2PRIO 2
##
## PHY2TAGS specifies whether or not tags will be removed
## from frames forwarded to the secondary (PC) Ethernet interface.
## Value Operation
##   0 Tags will be removed (default)
##   1 Tags will not be removed
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   Avaya Vantage Devices SIP R1.1.0.0 and later for K165/K175 models with embedded Ethernet switch
##   J129 SIP R1.0.0.0 and later
##   H1xx SIP R1.0 and later
##   96x1 SIP R6.3 and later
##   96x1 H.323 R6.6 and later
## SET PHY2TAGS 1
##
##### LAYER 3 QOS SETTINGS #####
##
## DSCPAUD specifies the layer 3 Differentiated Services (DiffServ) Code Point
## for audio frames generated by the telephone.
## Valid values are 0 through 63; the default value is 46.
## Note: This parameter may also be set via LLDP or H.323 signaling,
## which would overwrite any value set in this file.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0 and J100 SIP R2.0.0.0 and later
##   Avaya Vantage Basic Application SIP R1.1.0.1 and later; used in IP office environment only (for Aura environment
##   DSCPAUD is taken from PPM and configured using SMGR)
##   J129 SIP R1.0.0.0 and later
##   H1xx SIP R1.0 and later
##   96x1 H.323 R6.0 and later
##   96x1 SIP R6.0 and later
##   B189 H.323 R1.0 and later
##   96x0 H.323 R1.0 and later
##   96x0 SIP R1.0 and later
## SET DSCPAUD 43
##
##
## DSCPSIG specifies the layer 3 Differentiated Services (DiffServ) Code Point
## for signaling frames generated by the telephone.
## Valid values are 0 through 63; the default value is 34.
## Note: This parameter may also be set via LLDP or H.323 signaling,
## which would overwrite any value set in this file.

```



```

## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0 and J100 SIP R2.0.0.0 and later
## Avaya Vantage Basic Application SIP R1.1.0.1 and later; used in IP office environment only (for Aura environment
## DSCPSIG is taken from PPM and configured using SMGR)
## H1xx SIP R1.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## B189 H.323 R1.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## SET DSCPSIG 41
##
##### CALL QUALITY INDICATION SETTINGS #####
##
## WBCSTAT and QLEVEL_MIN configuration parameters related to the LOCAL network quality (MAY not be end to end indication).
##
## WBCSTAT specifies whether a wideband codec indication will be displayed when a wideband codec is being used
## Value Operation
## 0 Disabled
## 1 Enabled (default)
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 H.323 R6.4 and later
## 96x1 SIP R6.4 and later
## H1xx SIP R1.0 and later
## SET WBCSTAT 0
##
## QLEVEL_MIN specifies the minimum quality level for which a low local network quality indication will not be displayed
## Value Operation
## 1 Never display icon (default)
## 2 Packet loss is > 5% or round trip network delay is > 720ms or jitter compensation delay is > 160ms
## 3 Packet loss is > 4% or round trip network delay is > 640ms or jitter compensation delay is > 140ms
## 4 Packet loss is > 3% or round trip network delay is > 560ms or jitter compensation delay is > 120ms
## 5 Packet loss is > 2% or round trip network delay is > 480ms or jitter compensation delay is > 100ms
## 6 Packet loss is > 1% or round trip network delay is > 400ms or jitter compensation delay is > 80ms
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 H.323 R6.4 and later
## 96x1 SIP R6.4 and later
## H1xx SIP R1.0 and later
## SET QLEVEL_MIN 4
##
##### DHCP SETTINGS #####
##
## DHCPSTD specifies whether DHCP will comply with the IETF RFC 2131 standard and
## immediately stop using an IP address if the lease expires, or whether it will
## enter an extended rebinding state in which it continues to use the address and
## to periodically send a rebinding request, as well as to periodically send an
## ARP request to check for address conflicts, until a response is received from
## a DHCP server or until a conflict is detected.
## Value Operation
## 0 Continue using the address in an extended rebinding state (default).
## 1 Immediately stop using the address.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later
## H1xx SIP R1.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## B189 H.323 R1.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## SET DHCPSTD 1
##
## VLANTEST specifies the number of seconds that DHCP will be attempted with a
## non-zero VLAN ID before switching to a VLAN ID of zero (if the value of L2Q is 1)
## or to untagged frames (if the value of L2Q is 0).
## Valid values are 0 through 999; the default value is 60.

```

```

## A value of zero means that DHCP will try with a non-zero VLAN ID forever.
## This parameter is supported by:
## J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later (only J169/J179) - if L2QVLAN == 0, L2Q is treated as 2 (disabled).
## Avaya Vantage Devices SIP R1.0.0.0 and later. Note: L2Q==1 has the same behavior as L2Q==0.
## J129 SIP R1.0.0.0 and later
## H1xx SIP R1.0 and later. Note: L2Q==1 has the same behavior as L2Q==0.
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later. R7.1.0.0 and later, if L2QVLAN == 0, L2Q is treated as 2 (disabled).
## B189 H.323 R1.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## SET VLANTEST 90
##
## REUSETIME specifies the number of seconds that DHCP will be attempted with a VLAN ID of
## zero (if the value of L2Q is 1) or with untagged frames (if the value of L2Q is 0 or 2)
## before reusing the IP address (and associated address information) that it had the last
## time it successfully registered with a call server, if such an address is available.
## While reusing an address, DHCP will enter the extended rebinding state described above
## for DHCPSTD.
## Valid values are 0 and 20 through 999; the default value is 60.
## A value of zero means that DHCP will try forever (i.e., no reuse).
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## H1xx SIP R1.0 and later (REUSE mechanism is supported on Ethernet interface only (not Wi-Fi))
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## B189 H.323 R1.0 and later
## 96x0 H.323 R3.1 and later
## 96x0 SIP R2.5 and later
## SET REUSETIME 90
##
##### DNS SETTINGS #####
##
## DNSSRV specifies a list of DNS server addresses.
## Addresses can be in dotted-decimal (IPv4) or colon-hex (IPv6, if supported)
## format, separated by commas without any intervening spaces.
## A value set in this file will replace any value set for DNSSRV via DHCP.
## The value can contain 0 to 255 characters; the default value is null ("").
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later
## H1xx SIP R1.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## B189 H.323 R1.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## SET DNSSRV 198.152.15.15
##
## DOMAIN specifies a character string that will be appended to parameter values
## that are specified as DNS names, before the name is resolved.
## The value can contain 0 to 255 characters; the default value is null ("").
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later
## H1xx SIP R1.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## B189 H.323 R1.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## SET DOMAIN mycompany.com
##
##### GUEST LOGIN (AND VISITING USER) SETTINGS #####
##
## GUESTLOGINSTAT specifies whether the Guest Login feature is available to users.
## Value Operation

```

```

## 0 Guest Login feature is not available to users (default)
## 1 Guest Login feature is available to users
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later (J169 and J179 only)
## 96x1 H.323 R6.0 and later releases
## 96x0 H.323 R2.0 and later releases
## SET GUESTLOGINSTAT 0
##
## GUESTDURATION specifies the duration (in hours) before a Guest Login or a
## Visiting User login will be automatically logged off if the telephone is idle.
## Valid values are integers from 1 to 12, with a default value of 2.
## Note: Visiting user feature in this context related to H.323 endpoints using VUMCIPADD.
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later (J169 and J179 only)
## 96x1 H.323 R6.0 and later releases
## 96x0 H.323 R2.0 and later releases
## SET GUESTDURATION 2
##
## GUESTWARNING specifies the number of minutes before time specified by GUESTDURATION that
## a warning of the automatic logoff is initially presented to the Guest or Visiting User.
## Valid values are integers from 1 to 15, with a default value of 5.
## Note: Visiting user feature in this context related to H.323 endpoints using VUMCIPADD.
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later (J169 and J179 only)
## 96x1 H.323 R6.0 and later releases
## 96x0 H.323 R2.0 and later releases
## SET GUESTWARNING 5

##### SERVER SETTINGS (SIP) #####
## Note: Third party SIP call controllers (3PCC) support is only provided by J129 SIP R1.1.0.0, J100 SIP R2.0.0.0 and later.
##
## SIPDOMAIN specifies the domain name to be used during SIP registration.
## The value can contain 0 to 255 characters; the default value is null ("").
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Equinox 3.1.2 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later; not applicable when Avaya Vantage Open application is used.
## Avaya Vantage Basic Application SIP R1.0.0.0 and later; The configuration file from the Avaya Vantage Device
## include the highest precedence value from the following sources (High to low): UI, AADS, this file and PPM.
## J129 SIP R1.0.0.0 and later
## 96x1 SIP R6.0 and later
## 96x0 SIP R1.0 and later
## H1xx SIP R1.0 and later
## SET SIPDOMAIN example.com
##
##
## SIP_CONTROLLER_LIST specifies a list of SIP controller designators,
## separated by commas without any intervening spaces,
## where each controller designator has the following format:
## host[:port][:transport=xxx]
## host is an IP address in dotted-decimal (DNS name format is not supported unless stated otherwise below).
## [:port] is an optional port number.
## [:transport=xxx] is an optional transport type where xxx can be tls, tcp, or udp.
## If a port number is not specified a default value of 5060 for TCP and UDP or 5061 for TLS is used.
## If a transport type is not specified, a default value of tls is used.
## The value can contain 0 to 255 characters; the default value is null ("").
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0); J100 SIP R2.0.0.0 and later; DNS name format is supported for 3PCC environment only.
## For 3PCC environment, only one SIP controller is supported.
## J169/J179 SIP R1.5.0
## Avaya Equinox 3.1.2 and later; DNS name format is supported.
## Avaya Vantage Devices SIP R1.0.0.0 and later; DNS name format is supported; UDP is not supported; not applicable when Avaya
Vantage Open application is used.
## Avaya Vantage Basic Application SIP R1.0.0.0 and later; DNS name format is supported; UDP is not supported. The
## configuration file from the Avaya Vantage Device combines the configuration of this parameter from all sources (in the following
order):
## UI, LLDP, DHCP, this file, PPM and AADS.

```

```

## J129 SIP R1.0.0.0 and later; DNS name format is supported by J129 SIP R1.1.0.0 and later for 3PCC environment only. For
3PCC environment, only one SIP controller is supported.
## 96x1 SIP R6.0 and later
## 96x0 SIP R2.4.1 and later
## H1xx SIP R1.0 and later; udp is not supported.
## SET SIP_CONTROLLER_LIST proxy1:5555;transport=tls;proxy2:5556;transport=tls
##
## SIP_CONTROLLER_LIST_2
## Valid Values
## String The comma separated list of SIP proxy/registrar servers
## 0 to 255 characters: zero or more IP addresses in dotted decimal or colon-hex format,
## separated by commas without any intervening spaces.
## Default: "" (null)
## Description
## This parameter replaces SIP_CONTROLLER_LIST for dual mode phones. It is used to select the
## registration address.
## The list has the following format: host[:port][:transport=xxx]
## where:
## - host: is an IP addresses in dotted-decimal format or hex format
## - port: is the optional port number. If a port number is not specified the default
## value (5060 for TCP, 5061 for TLS) will be used
## - transport: is the optional transport type (where xxx is tls or tcp)
## If a transport type is not specified the default value TLS will be used
## A dual mode controller has addresses of both families within curly brackets.
## A settings file example is:
## SIP_CONTROLLER_LIST_2 "[{2007:7::5054:ff:fe35:c6e}:5060;transport=tcp, 47.11.15.142:5060;transport=tcp},
## {[2007:7::5054:ff:fe80:d4b0]:5060;transport=tcp, 47.11.15.174:5060;transport=tcp}"
## Dual mode phones use SIGNALING_ADDR_MODE to select SM IP addresses from SIP_CONTROLLER_LIST_2.
## If SIGNALING_ADDR_MODE is 4, register to the first IPv4 address in SIP_CONTROLLER_LIST_2.
## IPv4 only phones use SIP_CONTROLLER_LIST.
##
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## Example
## SET SIP_CONTROLLER_LIST_2 "[{2007:7::5054:ff:fe35:c6e}:5060;transport=tcp, 47.11.15.142:5060;transport=tcp},
## {[2007:7::5054:ff:fe80:d4b0]:5060;transport=tcp, 47.11.15.174 :5060;transport=tcp}"
##
## SIP Transport UDP
## Determines whether SIP Transport = UDP can be manually configured on the phone.
## 0 for No (default)
## 1 for Yes
## Note: This parameter is supported by J129 SIP R1.1.0.0 and J100 SIP R2.0.0.0 and later only for 3PCC environment.
## SET ENABLE_UDP_TRANSPORT 1
##
## SIPREGPROXYPOLICY specifies whether the telephone will attempt to maintain
## one or multiple simultaneous registrations.
## Value Operation
## alternate Only a single registration will be attempted and maintained.
## simultaneous Simultaneous registrations will be attempted and maintained with all available controllers.
## This parameter is supported by:
## J129 SIP R1.0.0.0 or R1.1.0.0, J100 SIP R2.0.0.0 and later, the default is simultaneous. The parameter shall be configured to
"alternate" in IP Office and 3PCC environments only.
## Not supported in 96x1 SIP R6.2 and later; the default value is simultaneous.
## 96x1 SIP R6.0.x; the default value is alternate.
## 96x0 SIP R2.4.1 and later; the default value is alternate.
## SET SIPREGPROXYPOLICY simultaneous
##
## SIMULTANEOUS_REGISTRATIONS specifies the number of Session Managers
## with which the telephone will simultaneously register.
## Valid values are 1, 2 or 3; the default value is 3.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Basic Application SIP R1.1.0.1 and later
## 96x1 SIP R6.0 and later
## 96x0 SIP R2.6 and later
## H1xx SIP R1.0 and later; For IP office environment this parameter shall be set to 1.
## SET SIMULTANEOUS_REGISTRATIONS 3

```

```

##
## CONNECTION_REUSE specifies whether the telephone will use two UDP/TCP/TLS connection (for both outbound
## and inbound) or one UDP/TCP/TLS connection.
## Value Operation
## 0 - disabled, the phone will open outbound connection to the SIP Proxy and listening socket for inbound connection
## from SIP proxy in parallel. This is the only and default behavior for pre-6.4 releases.
## 1 - enabled, the phone will not open a listening socket and will maintain and re-use the sockets it creates with
## the outbound proxies (default)
## For IP office environment this parameter shall be set to 1 (default).
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later, only value 1 is supported.
## 96x1 SIP R6.4 and later up to R7.1.0.0 (excluded) - values 0 and 1 are supported, R7.1.0.0 and later only value 1 is supported.
## H1xx SIP R1.0 and later
## SET CONNECTION_REUSE 0
##
##
## ENABLE_PPM_SOURCED_SIPPROXYSRVR parameter enables PPM as a source of SIP proxy server information.
## Value Operation
## 0 Proxy server information received from PPM will not be used.
## 1 Proxy server information received from PPM will be used (default).
## This parameter is not supported in IP Office environment as PPM is not supported.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## 96x0 SIP R2.4.1 and later
## H1xx SIP R1.0 and later
## SET ENABLE_PPM_SOURCED_SIPPROXYSRVR 1.
##
##
## CONFIG_SERVER_SECURE_MODE specifies whether HTTP or HTTPS is used to access the configuration server.
## Value Operation
## 0 use HTTP (default for 96x0 R2.0 through R2.5)
## 1 use HTTPS (default for other releases and products)
## 2 use HTTPS if SIP transport mode is TLS, otherwise use HTTP
## This parameter is not supported in IP Office environment as PPM is not supported.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R2.0 and later
## SET CONFIG_SERVER_SECURE_MODE 1
##
##
## VOLUME_UPDATE_DELAY specifies the minimum interval, in seconds, between backups of the volume levels to PPM service
## when the phone registered to Avaya Aura Session Manager. If no change to volume levels, there will be no backup to PPM service.
## Valid values are 2 through 900; the default value is 2.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.0.1 and later
## SET VOLUME_UPDATE_DELAY 20
##
##
##
## ENABLE_AVAYA_ENVIRONMENT specifies whether the telephone is configured
## for use in an Avaya (SES) or a third-party proxy environment.
## Value Operation
## 0 3rd party proxy with "SIPPING 19" features
## 1 Avaya SES with AST features and PPM (default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later; for IP office and 3PCC environments this parameter shall be set to 0.
## J169/J179 SIP R1.5.0
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later; for IP office environment this parameter shall be set to 0.
## 96x0 SIP R1.0 through R2.4
## SET ENABLE_AVAYA_ENVIRONMENT 1
##
##### NON-AVAYA ENVIRONMENT SETTINGS (SIP ONLY) #####
##

```

```

##
## DIALPLAN specifies the dial plan used in the telephone.
## It accelerates dialing by eliminating the need to wait for
## the INTER_DIGIT_TIMEOUT timer to expire.
## The value can contain 0 to 1023 characters; the default value is null ("").
## See the telephone Administrator's Guide for format and setting alternatives.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## 96x0 SIP R2.0 and later
## H1xx SIP R1.0 and later
## SET DIALPLAN [23]xxxx|91xxxxxxxxxx|9[2-9]xxxxxxxx
##
## PHNUMOFSA specifies the number of Session Appearances the telephone
## should support while operating in a non-Avaya environment.
## Valid values are 1 through 10; the default value is 3.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## 96x0 SIP R2.0 and later
## H1xx SIP R1.0 and later
## SET PHNUMOFSA 3

##### TIME SETTINGS (SIP ONLY) #####
##
## SNTPSVR specifies a list of addresses of SNTP servers.
## Addresses can be in dotted-decimal or DNS name format,
## separated by commas without any intervening spaces.
## The list can contain up to 255 characters; the default value is null ("").
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later
## 96x1 SIP R6.0 and later
## 96x0 SIP R1.0 and later
## H1xx SIP R1.0 and later
## SET SNTPSVR 192.168.0.5
##
## SNTP_SYNC_INTERVAL specifies the time interval in minutes at which the phone will attempt to synchronize its time with configured
NTP servers.
## Valid values: 60-2880 (minutes), Default: 1440 minutes (1 day).
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## SET SNTP_SYNC_INTERVAL 100
##
## GMTOFFSET specifies the time offset from GMT in hours and minutes.
## The format begins with an optional "+" or "-" ("+" is assumed if omitted),
## followed by 0 through 12 (hours), followed by a colon (:),
## followed by 00 through 59 (minutes). The default value is 0:00.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## H1xx SIP R1.0 only (TIMEZONE shall be used in R1.0.0.1 and later)
## 96x1 SIP R6.0 and later
## 96x0 SIP R1.0 and later
## SET GMTOFFSET 0:00
##
## DSTOFFSET specifies the time offset in hours of daylight savings time from local standard time.
## Valid values are 0, 1, or 2; the default value is 1.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## H1xx SIP R1.0 only (TIMEZONE shall be used in R1.0.0.1 and later)
## 96x1 SIP R6.0 and later
## 96x0 SIP R1.0 and later
## SET DSTOFFSET 1
##
## DSTSTART specifies when to apply the offset for daylight savings time.
## The default value for all telephones is 2SunMar2L

```

```

## (the second Sunday in March at 2AM local time).
## See the Administrator's Guide for format and setting alternatives.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## H1xx SIP R1.0 only (TIMEZONE shall be used in R1.0.0.1 and later)
## 96x1 SIP R6.0 and later
## 96x0 SIP R1.0 and later
## SET DSTSTART 2SunMar2L
##
## DSTSTOP specifies when to stop applying the offset for daylight savings time.
## The default value for all telephones is 1SunNov2L
## (the first Sunday in November at 2AM local time).
## See the Administrator's Guide for format and setting alternatives.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## H1xx SIP R1.0 only (TIMEZONE shall be used in R1.0.0.1 and later)
## 96x1 SIP R6.0 and later
## 96x0 SIP R1.0 and later
## SET DSTSTOP 1SunNov2L

##### TIMER SETTINGS (SIP ONLY) #####
##
## WAIT_FOR_REGISTRATION_TIMER specifies the number of seconds that the telephone will wait
## for a response to a REGISTER request. If no response message is received within this time,
## registration will be retried based on the value of RECOVERYREGISTERWAIT.
## Valid values are 4 through 3600; the default value is 32.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R2.5 and later
## Note: For Avaya Distributed Office configurations prior to R2.0, this parameter must be set to 60.
## SET WAIT_FOR_REGISTRATION_TIMER 60
##
## REGISTERWAIT specifies the number of seconds between re-registrations with the current server.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later; valid values are 30 to 86400; the default value is 900.
## Avaya Vantage Basic Application SIP R1.1.0.0 and later
## 96x1 SIP R6.0 and later; valid values are 30 to 86400; the default value is 900.
## H1xx SIP R1.0 and later; valid values are 30 to 86400; the default value is 900.
## 96x0 SIP R2.4.1 and later; valid values are 30 to 86400; the default value is 900.
## 96x0 SIP R1.0 through R2.2; valid values are 10 to 1000000000; the default value is 3600.
## SET REGISTERWAIT 1000
##

##
## WAIT_FOR_UNREGISTRATION_TIMER specifies the number of seconds that the telephone will wait
## before assuming that an un-registration request is complete.
## Un-registration includes termination of registration and all active dialogs.
## Valid values are 4 through 3600; the default value is 32.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R2.5 and later
## SET WAIT_FOR_UNREGISTRATION_TIMER 45
##
## WAIT_FOR_INVITE_RESPONSE_TIMEOUT specifies the maximum number of seconds that the
## telephone will wait for another response after receiving a SIP 100 Trying response.
## Valid values are 30 through 180; the default value is 60.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later.
## H1xx SIP R1.0 and later.
## SET WAIT_FOR_INVITE_RESPONSE_TIMEOUT 90
##
## OUTBOUND_SUBSCRIPTION_REQUEST_DURATION specifies the duration in seconds requested by the

```



```

## telephone in SUBSCRIBE messages, which may be decreased in the response from the server.
## Valid values are 60 through 31536000 (one year); the default value is 86400 (one day).
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   96x1 SIP R6.0 and later.
##   H1xx SIP R1.0 and later
##   96x0 SIP R2.0 and later.
## SET OUTBOUND_SUBSCRIPTION_REQUEST_DURATION 604800
##
## NO_DIGITS_TIMEOUT specifies the number of seconds that the telephone will wait
## for a digit to be dialed after going off-hook before generating a warning tone.
## Valid values are 1 through 60; the default value is 20.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   96x1 SIP R6.0 and later
##   H1xx SIP R1.0 and later
##   96x0 SIP R2.0 and later
## SET NO_DIGITS_TIMEOUT 15
##
## INTER_DIGIT_TIMEOUT specifies the number of seconds that the telephone will wait
## after a digit is dialed before sending a SIP INVITE.
## Valid values are 1 through 10; the default value is 5.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   96x1 SIP R6.0 and later
##   H1xx SIP R1.0 and later
##   96x0 SIP R2.0 and later
## SET INTER_DIGIT_TIMEOUT 6
##
## FAILED_SESSION_REMOVAL_TIMER specifies the number of seconds the telephone will
## display a session line appearance and generate re-order tone after an invalid
## extension has been dialed if the user does not press the End Call softkey.
## Valid values are 5 through 999; the default value is 30.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   96x1 SIP R6.0 and later
##   H1xx SIP R1.0 and later
##   96x0 SIP R1.0 and later
## SET FAILED_SESSION_REMOVAL_TIMER 15
##
## TCP_KEEP_ALIVE_STATUS specifies whether or not the telephone sends TCP keep alive messages.
## Value Operation
## 0 Keep-alive messages are not sent
## 1 Keep-alive messages are sent (default)
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   96x1 SIP R6.0 and later
##   H1xx SIP R1.0 and later
##   96x0 SIP R1.0 and later
## SET TCP_KEEP_ALIVE_STATUS 0
##
## TCP_KEEP_ALIVE_TIME specifies the number of seconds that the telephone will wait
## before sending out a TCP keep-alive (TCP ACK) message.
## Valid values are 10 through 3600; the default value is 60.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   96x1 SIP R6.0 and later
##   H1xx SIP R1.0 and later
##   96x0 SIP R1.0 and later
## SET TCP_KEEP_ALIVE_TIME 45
##
## TCP_KEEP_ALIVE_INTERVAL specifies the number of seconds that the telephone will wait
## before re-transmitting a TCP keep-alive (TCP ACK) message.
## Valid values are 5 through 60; the default value is 10.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   96x1 SIP R6.0 and later
##   H1xx SIP R1.0 and later

```



```

## 96x0 SIP R1.0 and later
## SET TCP_KEEP_ALIVE_INTERVAL 15
##
## CONTROLLER_SEARCH_INTERVAL specifies the number of seconds the telephone will wait
## to complete the maintenance check for monitored controllers.
## Valid values are 4 through 3600.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later (default value is 16)
## 96x1 SIP R6.0 and later (default value is 16)
## H1xx SIP R1.0 and later (default value is 16)
## 96x0 SIP R2.6.5 and later (default value is 16)
## 96x0 SIP R2.4.1 - R2.6.4 (default value is 4)
## SET CONTROLLER_SEARCH_INTERVAL 20
##
## ASTCONFIRMATION specifies the number of seconds that the telephone will wait to validate
## an active subscription when it SUBSCRIBES to the "avaya-cm-feature-status" package.
## Valid values are 16 through 3600.
## This parameter is not supported in IP Office and 3PCC environments as there is no subscription to avaya-cm-feature-status.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later; the default value is 32.
## 96x1 SIP R6.0 and later; the default value is 32.
## H1xx SIP R1.0 and later; the default value is 32.
## 96x0 SIP R2.6 and later; the default value is 60.
## SET ASTCONFIRMATION 90
##
## FAST_RESPONSE_TIMEOUT specifies the number of seconds that the telephone will wait
## before terminating an INVITE transaction if no response is received.
## However, a value of 0 means that this timer is disabled.
## Valid values are 0 through 32; the default value is 4.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later - it is provided by SMGR for phones connected to Avaya Aura however the
settings file
## configuration is still applicable for non-Avaya Aura systems.
## 96x1 SIP 6.0 and later. In 96x1 SIP R6.2 it is provided by SMGR for phones connected to Avaya Aura however the settings file
## configuration is still applicable for non-Avaya Aura systems.
## 96x0 SIP R2.4.1 and later
## SET FAST_RESPONSE_TIMEOUT 5
##
## RDS_INITIAL_RETRY_TIME specifies the number of seconds that the telephone will wait
## the first time before trying to contact the PPM server again after a failed attempt.
## Each subsequent retry will be delayed by double the previous delay.
## Valid values are 2 through 60, the default value is 2.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R2.4.1 and later
## SET RDS_INITIAL_RETRY_TIME 4
##
## RDS_MAX_RETRY_TIME specifies the maximum delay interval in seconds after which
## the telephone will abandon its attempt to contact the PPM server.
## Valid values are 2 through 3600, the default value is 600.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R2.4.1 and later
## SET RDS_MAX_RETRY_TIME 600
##
## RDS_INITIAL_RETRY_ATTEMPTS specifies the number of retries after which
## the telephone will abandon its attempt to contact the PPM server.
## Valid values are 1 through 30, the default value is 15.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R2.4.1 and later
## SET RDS_INITIAL_RETRY_ATTEMPTS 20

```

```

##
## SIP Timer T1 is an estimate of the Round Trip Time (RTT) and is defined in milliseconds.
## Valid values are 500 through 10000 milliseconds; the default value is 500.
## Note: This parameter is supported by J129 SIP R1.1.0.0 and J100 SIP R2.0.0.0 and later only for 3PCC environment.
## SET SIP_TIMER_T1 2000
##
## SIP Timer T2 is maximum retransmit interval for non-INVITE requests and INVITE responses and is defined in milliseconds.
## Valid values are 2000 through 40000 milliseconds; the default value is 4000.
## Note: This parameter is supported by J129 SIP R1.1.0.0 and J100 SIP R2.0.0.0 and later only for 3PCC environment.
## SET SIP_TIMER_T2 5000
##
## SIP Timer T4 is maximum duration a message will remain in the network and is defined in milliseconds.
## Valid values are 2500 through 60000 milliseconds; the default value is 5000.
## Note: This parameter is supported by J129 SIP R1.1.0.0 and J100 SIP R2.0.0.0 and later only for 3PCC environment.
## SET SIP_TIMER_T4 6000
##
##
## FORBIDDEN_SESSION_REMOVAL_TIMER specifies the duration of an off-hook
## session before call is automatically ended in case no more call appearances
## is available on the called/remote party.
## Value: 5 - 20 seconds; Default 10 seconds
## This parameter is supported by:
##     J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0 and J100 SIP R2.0.0.0 and later
##     96x1 SIP R7.1.0.0 and later
## SET FORBIDDEN_SESSION_REMOVAL_TIMER 5
##
##### CONFERENCING SETTINGS (SIP ONLY) #####
##
## CONFERENCE_FACTORY_URI specifies the URI for Avaya Aura Conferencing or Network Conferencing in 3PCC environments.
## Valid values contain zero or one URI,
## where a URI consists of a dial string followed by "@" followed by a domain,
## which must match the routing pattern configured in System Manager for Adhoc Conferencing.
## Depending on the dial plan, the dial string may need a prefix code, such as a 9 to get an outside line.
## The domain portion of the URI can be in the form of an IP address or an FQDN.
## The value can contain 0 to 255 characters; the default value is null ("").
## This parameter is supported by:
##     J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##     Avaya Equinox 3.1.2 and later
##     96x1 SIP R6.2.1 and later
##     H1xx SIP R1.0 and later
## SET CONFERENCE_FACTORY_URI "93375000@avaya.com"
##
##
## EVENT_NOTIFY_AVAYA_MAX_USERS specifies the maximum number of users to be included in
## an event notification message from CM/AST-II or Avaya Aura Conferencing R6.0 or later.
## Valid values are 0 through 1000; the default value is 20.
## It is used only for development and debugging purposes.
## This parameter is supported by:
##     J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##     96x1 SIP R6.2 and later
## SET EVENT_NOTIFY_AVAYA_MAX_USERS 10
##
##### PRESENCE SETTINGS (SIP ONLY) #####
##
## ENABLE_PRESENCE specifies whether presence will be supported.
## Value Operation
## 0 Disabled
## 1 Enabled
## This parameter is supported by:
##     J129 SIP R1.0.0.0 (or R1.1.0.0) and J100 SIP R2.0.0.0 and later (default is 1); For IP office and 3PCC environments this parameter
##     shall be set to 0 as presence is not supported.
##     J169/J179 SIP R1.5.0 (default is 1)
##     96x1 SIP R6.2 and later (default is 1)
##     96x0 SIP R2.6.8 and later (default is 1)
##     96x0 SIP R2.6.6 and R2.6.7 (default is 0)
##     H1xx SIP R1.0 and later (default is 1); For IP office environment this parameter shall be set to 0 as presence is not supported.
## SET ENABLE_PRESENCE 1

```

```

##
## ALLOW_DND_SAC_LINK_CHANGE determines if the user will be allowed to change the DND and SAC button link.
## If the change is allowed, the menu to set the DND and SAC link is displayed.
## Value Operation
## 0 - do not allow a user to change default behavior (Default)
## 1 - allow a user change default behavior; parameter will be included in the "A" menu
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R6.4 and later.
## SET ALLOW_DND_SAC_LINK_CHANGE 1
##
## DND_SAC_LINK defines link between the DND and SAC buttons. The value of this parameter is used if the
## ALLOW_DND_SAC_LINK_CHANGE is set to 0.
## Value Operation
## 0 - enabling DND will not enable SAC (default)
## 1 - enabling DND will enable SAC
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R6.4 and later.
## SET DND_SAC_LINK 1

##
## PRESENCE_ACL_CONFIRM specifies the handling of a Presence ACL update with pending watchers.
## Value Operation
## 0 Auto confirm - automatically send a PUBLISH to allow presence monitoring (Default)
## 1 Ignore - take no action
## 2 Prompt - the phone directly prompting the user to Allow or Deny the watcher's request.
## This parameter is not supported in IP Office environment as presence is not supported.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0 and J100 SIP R2.0.0.0 and later (values 0-1)
## 96x1 SIP R6.3 and later (values 0-1)
## H1xx SIP R1.0 and later (values 0-2)
## SET PRESENCE_ACL_CONFIRM 1
##

##### MLPP SETTINGS (SIP ONLY) #####
##
## ENABLE_MLPP specifies whether MLPP feature is enabled or not.
## Value Operation
## 0 Disable MLPP feature (default)
## 1 Enable MLPP feature
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R7.1.0.0 and later
## SET ENABLE_MLPP 1
##
## MLPP_NET_DOMAIN specifies MLPP Network Domain
## Value Operation
## "" No MLPP Network Domain is configured (default)
## "dsn" DSN Network
## "uc" UC Network
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R7.1.0.0 and later
## SET MLPP_NET_DOMAIN "dsn"
##
## MLPP_MAX_PREC_LEVEL specifies maximum allowed precedence level for the user
## Value Operation
## 1 Maximum allowed precedence level is Routine (default)
## 2 Maximum allowed precedence level is Priority
## 3 Maximum allowed precedence level is Immediate
## 4 Maximum allowed precedence level is Flash
## 5 Maximum allowed precedence level is Flash Override
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R7.1.0.0 and later
## SET MLPP_MAX_PREC_LEVEL 2
##

```

```

## ENABLE_PRECEDENCE_SOFTKEY indicates whether precedence soft key should be enabled on idle line appearances on Phone Screen.
## Value Operation
## 0 Disable precedence soft key
## 1 Enable precedence soft key (default)
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R7.1.0.0 and later
## SET ENABLE_PRECEDENCE_SOFTKEY 0
##
## DSCPAUD_FO specifies the DSCP value for Flash Override precedence/priority level voice call (0-63). Default value is 41.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R7.1.0.0 and later
## SET DSCPAUD_FO 42
##
## DSCPAUD_FL specifies the DSCP value for Flash precedence/priority level voice call (0-63). Default value is 43.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R7.1.0.0 and later
## SET DSCPAUD_FL 44
##
## DSCPAUD_IM specifies the DSCP value for Immediate precedence/priority level voice call (0-63). Default value is 45.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R7.1.0.0 and later
## SET DSCPAUD_IM 43
##
## DSCPAUD_PR specifies the DSCP value for Priority precedence/priority level voice call (0-63). Default value is 47.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R7.1.0.0 and later
## SET DSCPAUD_PR 48
##
## DSCPMGMT specifies the DSCP value for OA&M management packet (0-63). The default value is 16.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R7.1.0.0 and later
## SET DSCPMGMT 15
##
##### EXCHANGE SETTINGS (SIP ONLY) #####
##
## EXCHANGE_SERVER_LIST specifies a list of one or more Exchange server IP addresses.
## Addresses can be in dotted-decimal or DNS name format,
## separated by commas without any intervening spaces.
## The list can contain up to 255 characters; the default value is null ("").
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R6.0 and later
## 96x0 SIP R2.5 and later
## H1xx SIP R1.0 and later
## SET EXCHANGE_SERVER_LIST exch1.myco.com,exch2.myco.com,exch3.myco.com
##
##
## PROVIDE_EXCHANGE_CONTACTS specifies whether menu item(s) for Exchange Contacts are displayed.
## Value Operation
## 0 Not displayed
## 1 Displayed (default)
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R6.2 and later
## 96x0 SIP R2.0 through R2.4 only
## SET PROVIDE_EXCHANGE_CONTACTS 0
##
## PROVIDE_EXCHANGE_CALENDAR specifies whether menu item(s) for Exchange Calendar are displayed.
## Value Operation
## 0 Not displayed
## 1 Displayed (default)

```

```

## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later (J169/J179 only)
##   96x1 SIP R6.0 and later
##   96x0 SIP R2.5 and later
## SET PROVIDE_EXCHANGE_CALENDAR 0
##

##
## EXCHANGE_USER_DOMAIN specifies the domain for the URL
## used to obtain Exchange contacts and calendar data. The EXCHANGE_USER_DOMAIN is used as part of the
## user authentication.
## The value can contain 0 to 255 characters; the default value is null ("").
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later (J169/J179 only); Users can change this value in the "Options & Settings...". Refer to
EXCHANGE_AUTH_USERNAME_FORMAT for how EXCHANGE_USER_DOMAIN is used.
##   J169/J179 SIP R1.5.0; Users can change this value in the "Options & Settings...". Refer to EXCHANGE_AUTH_USERNAME_FORMAT
for how EXCHANGE_USER_DOMAIN is used.
##   96x1 SIP R6.0 and later; Users can change this value in the "Options & Settings...". Refer to
EXCHANGE_AUTH_USERNAME_FORMAT for how EXCHANGE_USER_DOMAIN is used.
##   H1xx SIP R1.0 and later
##   96x0 SIP R2.5 and later
## SET EXCHANGE_USER_DOMAIN exchange.myco.com
##
## EXCHANGE_AUTH_USERNAME_FORMAT specifies the format of the username for user authentication.
## Value Operation
## 0 Office 2003/Office2016 username format - "EXCHANGE_USER_DOMAIN\Exchange Username" or "Exchange Username" if
EXCHANGE_USER_DOMAIN is "".
## This is the default value.
## 1 Office 365 username format - "Exchange Username@EXCHANGE_USER_DOMAIN" or "Exchange Username" if
EXCHANGE_USER_DOMAIN is "".
## This parameter is supported by:
##   J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later
##   96x1 SIP R7.1.0.0 and later.
## SET EXCHANGE_AUTH_USERNAME_FORMAT 1
##
## EXCHANGE_EMAIL_DOMAIN specifies the Exchange email domain.
## Exchange Username with EXCHANGE_EMAIL_DOMAIN defines the email address: Exchange
Username@EXCHANGE_EMAIL_DOMAIN.
## This parameter cannot be changed by end users in the "Options & Settings..." menu.
## The value can contain 0 to 255 characters; the default value is null ("").
## This parameter is supported by:
##   J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
##   96x1 SIP R6.3 and later
## SET EXCHANGE_EMAIL_DOMAIN avaya.com
##
## ENABLE_EXCHANGE_REMINDER specifies whether or not Exchange reminders will be displayed.
## Value Operation
## 0 Not displayed (default)
## 1 Displayed
## This parameter is supported by:
##   J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
##   96x1 SIP R6.0 and later
##   96x0 SIP R2.5 and later
## SET ENABLE_EXCHANGE_REMINDER 1
##
## EXCHANGE_REMINDER_TIME specifies the number of minutes before an appointment
## at which a reminder will be displayed.
## Valid values are 0 through 60; the default value is 5.
## This parameter is supported by:
##   J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
##   96x1 SIP R6.0 and later
##   96x0 SIP R2.5 and later
## SET EXCHANGE_REMINDER_TIME 7
##
## EXCHANGE_SNOOZE_TIME specifies the number of minutes after a reminder has been
## temporarily dismissed at which the reminder will be redisplayed.
## Valid values are 0 through 60; the default value is 5.
## This parameter is supported by:

```

```

## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R6.0 and later
## 96x0 SIP R2.5 and later
## SET EXCHANGE_SNOOZE_TIME 4
##
## EXCHANGE_REMINDER_TONE specifies whether or not a tone will be generated
## the first time an Exchange reminder is displayed.
## Value Operation
## 0 Tone not generated
## 1 Tone generated (default)
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R6.0 and later
## 96x0 SIP R2.5 and later
## SET EXCHANGE_REMINDER_TONE 0
##
## EXCHANGE_NOTIFY_SUBSCRIPTION_PERIOD specifies the number of seconds between re-syncs
## with the Exchange server.
## This parameter is supported by:
## J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later (J169/J179 only); valid values are 60 through 3600; the default value is 180.
## 96x1 SIP R6.2 and later; valid values are 60 through 3600; the default value is 180.
## 96x1 SIP R6.0.x; valid values are 0 through 3600; the default value is 180.
## 96x0 SIP R2.5 and later; valid values are 0 through 3600; the default value is 180.
## SET EXCHANGE_NOTIFY_SUBSCRIPTION_PERIOD 200

```

OTHER SIP-ONLY SETTINGS

```

##
## SPEAKERSTAT specifies the operation of the speakerphone.
## Value Operation
## 0 Speakerphone disabled
## 1 One-way speaker (also called "monitor") enabled
## 2 Full (two-way) speakerphone enabled (default)
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## 96x0 SIP R1.0 and later
## SET SPEAKERSTAT 1
##
## MUTE_ON_REMOTE_OFF_HOOK controls the speakerphone muting for a remote-initiated
## (a shared control or OOD-REFER) speakerphone off-hook.
##
## Valid values are 0 and 1
## 0 - the speakerphone is Unmuted
## 1 - the speakerphone is Muted
##
## The default value is 1 (Muted) for 96x1 SIP R6.3
## The default value is 0 (Unmuted) for 96x1 SIP R6.3.1 and later, J129 SIP R1.0.0.0 and later and H1xx SIP R1.0 and later
##
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.3 and later
## 96x1 SIP R6.3 and later
## H1xx SIP R1.0 and later; R1.0.2 and later - this parameter is also supported in IPO environment where it is used
## to control auto answer calls whether they start muted (1) or not (0).
##
## The value of the parameter MUTE_ON_REMOTE_OFF_HOOK will be applied to the phone only when the phone is
## deployed with a CM 6.2.2 and earlier releases.
##
## If the phone is deployed with CM 6.3 or later, the MUTE_ON_REMOTE_OFF_HOOK variable is ignored and instead
## the feature is delivered via PPM by enabling the Turn on mute for remote off-hook attempt parameter in the station form
## via the Session Manager (System Manager) or Communication Manager (SAT) administrative interfaces.
##
## SET MUTE_ON_REMOTE_OFF_HOOK 0
##
##
##
## SDPCAPNEG specifies whether or not SDP capability negotiation is enabled.

```

```

## Value Operation
## 0 SDP capability negotiation is disabled
## 1 SDP capability negotiation is enabled (default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R2.6 and later
## SET SDPCAPNEG 0
##
## ENFORCE_SIPS_URI specifies whether a SIPS URI must be used for SRTP.
## Value Operation
## 0 Not enforced
## 1 Enforced (default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0) and J100 SIP R2.0.0.0 and later; not applicable for 3PCC environment
## J169/J179 SIP R1.5.0
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R2.6 and later
## SET ENFORCE_SIPS_URI 1
##
## 100REL_SUPPORT specifies whether the 100rel option tag is included in the SIP INVITE header field.
## Value Operation
## 0 The tag will not be included.
## 1 The tag will be included (default).
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R2.6 and later
## SET 100REL_SUPPORT 1
##
## PLAY_TONE_UNTIL_RTP specifies whether locally-generated ringback tone will stop
## as soon as SDP is received for an early media session, or whether it will continue
## until RTP is actually received from the far-end party.
## Value Operation
## 0 Stop ringback tone as soon as SDP is received
## 1 Continue ringback tone until RTP is received (default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.2 and later
## H1xx SIP R1.0 and later
## SET PLAY_TONE_UNTIL_RTP 0
##
## TEAM_BUTTON_RING_TYPE specifies the alerting pattern to use for team buttons.
## Valid values are 1 through 8, the default value is 1.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R6.2 and later
## SET TEAM_BUTTON_RING_TYPE 3
##
## LOCALLY_ENFORCE_PRIVACY_HEADER specifies whether the telephone will display
## "Restricted" (in the current language) instead of CallerId information when
## a Privacy header is received in a SIP INVITE message for an incoming call.
## Value Operation
## 0 Disabled (default): CallerID information will be displayed
## 1 Enabled: "Restricted" will be displayed
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.2 and later
## H1xx SIP R1.0 and later
## SET LOCALLY_ENFORCE_PRIVACY_HEADER 1
##
## ENABLE_SIP_USER_ID controls the display of the user ID input field on the Login Screen

```



```

## Value Operation
## 0 SIP User ID field is not available to user during Login default)
## 1 SIP User ID field is available to user during Login
## Note: This parameter is supported by J129 SIP R1.1.0.0 and J100 SIP R2.0.0.0 and later only for 3PCC environment.
## SET ENABLE_SIP_USER_ID 1
##
## ENABLE_STRICT_USER_VALIDATION specifies whether AOR received in 'Request-URI' of incoming call should be validated or not
## with 'contact' header published by phone in REGISTRATION.
## Value Operation
## 0 validation is not done (Default)
## 1 validation is done
## Note: This parameter is supported by J129 SIP R1.1.0.0 and J100 SIP R2.0.0.0 and later only for 3PCC environment.
## SET ENABLE_STRICT_USER_VALIDATION 1
##
## BRANDING_VOLUME specifies the volume level at which the Avaya audio brand is played.
## Value Operation
## 8 9db above nominal
## 7 6db above nominal
## 6 3db above nominal
## 5 nominal (default)
## 4 3db below nominal
## 3 6db below nominal
## 2 9db below nominal
## 1 12db below nominal
## 0 No Volume
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later (Values 0-8)
## J169/J179 SIP R1.5.0 (Values 1-8)
## Avaya Vantage Devices SIP R1.0.0.0 and later (Values 1-8)
## J129 SIP R1.0.0.0 (or R1.1.0.0) (Values 1-8)
## 96x1 SIP R6.2 and later (Values 1-8)
## H1xx SIP R1.0 and later (Values 1-8)
## SET BRANDING_VOLUME 2
##
## ENABLE_OOD_MSG_TLS_ONLY specifies whether an Out-Of-Dialog (OOD) REFER
## must be received over TLS transport to be accepted.
## Value Operation
## 0 No, TLS is not required
## 1 Yes, TLS is required (default)
## Note: A value of 0 is only intended for testing purposes.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0 and J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.2 and later
## H1xx SIP R1.0 and later
## SET ENABLE_OOD_MSG_TLS_ONLY 1
##
## TEAM_BUTTON_REDIRECT_INDICATION controls if the redirection indication should be shown on
## a Team Button (on a monitoring station) in case it is not a redirect destination of the monitored station.
## Value Operation
## 0 - disabled; the redirect indication will be shown only on a monitoring station which is redirection destination (default).
## 1 - enabled; the redirection icon is displayed on all monitoring stations
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R6.4 and later
## SET TEAM_BUTTON_REDIRECT_INDICATION 1
##
## ENABLE_BLIND_TRANSFER indicates whether enable blind transfer or not
## Value Operation
## 0 Disable blind transfer
## 1 Enable blind transfer (default)
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R7.1.0.0 and later
## SET ENABLE_BLIND_TRANSFER 0
##
##### ACCESSIBILITY SETTINGS (SIP ONLY) #####
##

```


PROVIDE_KEY_REPEAT_DELAY specifies how long a navigation button must be held down before it begins to auto-repeat, and whether an option will be provided by which the user can change this value.

Value Operation

0 Default (500ms) with user option (default)

1 Short (250ms) with user option

2 Long (1000ms) with user option

3 Very Long (2000ms) with user option

4 No Repeat with user option

5 Default (500ms) without user option

6 Short (250ms) without user option

7 Long (1000ms) without user option

8 Very Long (2000ms) without user option

9 No Repeat without user option

This parameter is supported by:

J169/J179 SIP R1.5.0; **J100 SIP R2.0.0.0 and later (J169/J179 only)**

96x1 SIP R6.2 and later

SET PROVIDE_KEY_REPEAT_DELAY 2

HEADSET PROFILES

##

HEADSET_PROFILE_DEFAULT specifies the number of the default headset audio profile.

Valid values are 1 through 20; the default value is 1.

This parameter is supported by:

J169/J179 SIP R1.5.0; **J100 SIP R2.0.0.0 and later (J169/J179 only)**

Avaya Vantage Devices SIP R1.0.0.0 and later

96x1 SIP R6.3 and later.

H1xx SIP R1.0 and later

SET HEADSET_PROFILE_DEFAULT 1

##

HEADSET_PROFILE_NAMES specifies an ordered list of names to be displayed for headset audio profile selection.

The list can contain 0 to 255 UTF-8 characters; the default value is null ("").

Names are separated by commas without any intervening spaces.

Two commas in succession indicate a null name,

which means that the default name should be displayed for the corresponding profile.

Names may contain spaces, but if any do, the entire list must be quoted.

There is no way to prevent a profile from being displayed.

This parameter is supported by:

J169/J179 SIP R1.5.0; **J100 SIP R2.0.0.0 and later (J169/J179 only)**

Avaya Vantage Devices SIP R1.0.0.0 and later

96x1 SIP R6.3 and later.

H1xx SIP R1.0 and later

SET HEADSET_PROFILE_NAMES "Acme Earwigs,,Spinco Ear Horns"

##

HANDSET PROFILES

##

HANDSET_PROFILE_DEFAULT specifies the number of the default handset audio profile.

Valid values are 1 through 20; the default value is 1.

This parameter is supported by:

J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, **J100 SIP R2.0.0.0 and later**

Avaya Vantage Devices SIP R1.0.0.0 and later

SET HANDSET_PROFILE_DEFAULT 1

##

HANDSET_PROFILE_NAMES specifies an ordered list of names to be displayed for handset audio profile selection.

The list can contain 0 to 255 UTF-8 characters; the default value is null ("").

Names are separated by commas without any intervening spaces.

Two commas in succession indicate a null name,

which means that the default name should be displayed for the corresponding profile.

Names may contain spaces, but if any do, the entire list must be quoted.

There is no way to prevent a profile from being displayed.

This parameter is supported by:

J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, **J100 SIP R2.0.0.0 and later**

Avaya Vantage Devices SIP R1.0.0.0 and later

SET HANDSET_PROFILE_NAMES "Acme Earwigs,,Spinco Ear Horns"

##

EMERGENCY TELEPHONE NUMBER

##

PHNEMERGNUM specifies an emergency telephone number to be dialed if the associated button is selected.

```
## Valid values may contain up to 30 dialable characters (0-9, *, #); the default value is null ("").
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.1.0.1 and later for IP Office Environment only
## 96x1 H.323 R6.0 and later; the parameter is supported when the phone is registered to Avaya Communication Manager only.
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## B189 H.323 R1.0 and later
## 96x0 H.323 R1.5 and later; the parameter is supported when the phone is registered to Avaya Communication Manager only.
## 96x0 SIP R2.0 and later
## 4630 H.323 R1.0 and later
## SET PHNEMERGNUM 9911
##
##
## PHNMOREEMERGNUMS specifies list of comma separated emergency numbers
## Valid values may contain up to 30 dialable characters (0-9, *, #); the default value is null ("").
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.1.0.1 and later for IP Office Environment only
## H1xx SIP R1.0.2 and later
## SET PHNMOREEMERGNUMS "911,109,115"
```

```
##### EMERGENCY NUMBER SOFTKEY (SIP ONLY) #####
##
## ENABLE_SHOW_EMERG_SK specifies whether an emergency softkey,
## with or without a confirmation screen, will be displayed when the phone is registered.
## All emergency numbers will always be supported.
## Value Operation
## 0 An emergency softkey will not be displayed.
## 1 An emergency softkey will be displayed, without a confirmation screen.
## 2 An emergency softkey will be displayed, with a confirmation screen (default).
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.2 and later
## SET ENABLE_SHOW_EMERG_SK 1
##
## ENABLE_SHOW_EMERG_SK_UNREG specifies whether an emergency softkey,
## with or without a confirmation screen, will be displayed when the phone is not registered.
## All emergency numbers will always be supported.
## Value Operation
## 0 An emergency softkey will not be displayed.
## 1 An emergency softkey will be displayed, without a confirmation screen.
## 2 An emergency softkey will be displayed, with a confirmation screen (default).
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.2 and later
## SET ENABLE_SHOW_EMERG_SK_UNREG 1
##
```

```
##### CALL LOG SETTINGS #####
##
```

```
##
## LOG_DIALED_DIGITS specifies if the call log will contain digits dialed by a user or
## information about a remote party in case where the user dialed a FAC code.
## The FAC code is identified by * or # entered as a first character.
##
## Value Operation
## 0 Allow dialed FAC code to be replaced with a remote party number in the call History
## 1 Dialed digits are logged in call History exactly as they were entered by the user (default).
##
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.5 and later
## SET LOG_DIALED_DIGITS 0
##
```

```

##### CALL CENTER SETTINGS #####
##
## HEADSYS specifies whether the telephone will go on-hook if the headset is active
## when a Disconnect message is received.
## Value Operation
## 0 The telephone will go on-hook if a Disconnect message is received when the headset is active
## 1 Disconnect messages are ignored when the headset is active
## Note: a value of 2 has the same effect as a value of 0, and
## a value of 3 has the same effect as a value of 1.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only) (the default value is 0)
## 96x1 H.323 R6.2.1 and later (the default value is 0 unless the value
## of CALLCTRSTAT is set to 1, in which case the default value is 1)
## 96x1 H.323 R6.1 and R6.2 ignore this parameter, and will ignore Disconnect messages
## if the user is logged in as a call center agent. If the user is not logged in
## as a call center agent, the telephone will go on-hook if a Disconnect message
## is received when the headset is active.
## 96x1 H.323 releases prior to R6.1 (the default value is 1)
## 96x1 SIP R6.4 and later (the default value is 0)
## 96x1 SIP R6.0 and later up to R6.4 (not included) (the default value is 1)
## 96x0 H.323 R1.2 and later (the default value is 1)
## 96x0 SIP R1.0 and later (the default value is 1)
## SET HEADSYS 0
##
##### CALL CENTER SETTINGS (96x1 SIP ONLY) #####
##
## SKILLSCREENTIME specifies the duration, in seconds, that the Skills screen will be displayed.
## Valid values are 0 through 60; the default value is 5.
## A value of 0 means that the Skills screen will not be removed automatically when the agent logs in.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R6.2 and later
## SET SKILLSCREENTIME 5
##
## UIDISPLAYTIME specifies the duration, in seconds, that the UUI Information screen will be displayed.
## Valid values are 5 through 60; the default value is 10.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R6.2 and later
## SET UIDISPLAYTIME 10
##
## ENTRYNAME specifies whether the Calling Party Name or the VDN/Skill Name will be used in History entries.
## Value Operation
## 0 Calling Party Name will be used (default)
## 1 VDN/Skill Name will be used
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R6.2 and later
## SET ENTRYNAME 1
##
## CC_INFO_TIMER specifies the duration, in hours, of the subscription to the SIP CC-Info event package.
## Valid values are 1 through 24; the default value is 8.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R6.2 and later
## SET CC_INFO_TIMER 8
##
##### RECORDING TONE SETTINGS (96x1 H.323 and SIP ONLY) #####
##
## RECORDINGTONE specifies whether Call Recording Tone will be generated on active calls.
## Value Operation
## 0 Call Recording Tone will not be generated (default)
## 1 Call Recording Tone will be generated
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R7.0.0 and later
## 96x1 H.323 R6.2 and later

```

```

## B189 H.323 R1.0 and later
## SET RECORDINGTONE 1
##
## RECORDINGTONE_INTERVAL specifies the number of seconds between Call Recording Tones.
## Valid values are 1 through 60; the default value is 15.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R7.0.0 and later
## 96x1 H.323 R6.2 and later
## B189 H.323 R1.0 and later
## SET RECORDINGTONE_INTERVAL 10
##
## RECORDINGTONE_VOLUME specifies the volume of the Call Recording Tone in 5dB steps.
## Value Operation
## 0 The tone volume is equal to the transmit audio level (default)
## 1 The tone volume is 45dB below the transmit audio level
## 2 The tone volume is 40dB below the transmit audio level
## 3 The tone volume is 35dB below the transmit audio level
## 4 The tone volume is 30dB below the transmit audio level
## 5 The tone volume is 25dB below the transmit audio level
## 6 The tone volume is 20dB below the transmit audio level
## 7 The tone volume is 15dB below the transmit audio level
## 8 The tone volume is 10dB below the transmit audio level
## 9 The tone volume is 5dB below the transmit audio level
## 10 The tone volume is equal to the transmit audio level
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R7.0.0 and later
## 96x1 H.323 R6.2 and later
## B189 H.323 R1.0 and later
## SET RECORDINGTONE_VOLUME 8

##### TRUSTED CERTIFICATES AND GENERAL CERTIFICATES SETTINGS #####
##
## TRUSTCERTS specifies a list of names of files that contain copies of CA certificates
## (in PEM format) that will be downloaded, saved in non-volatile memory,
## and used by the telephone to authenticate received identity certificates.
## The list can contain up to 255 characters.
## Values are separated by commas without intervening spaces.
## The default value is null ("").
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later; support of up to 100 PEM and DER format root and intermediate trusted certificates.
## The list can contain up to 1024 characters. Avaya Vantage Open application does not use the downloaded trusted
certificates.
## However, when Avaya Vantage Open application is installed, this parameter is used to download trusted certificates for
## to be used Avaya Vantage device (for example, 802.1x EAP-TLS) or by other applications (for example, Android Browser, etc.).
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## B189 H.323 R1.0 and later
## 96x0 H.323 R2.0 and later
## 96x0 SIP R1.0 and later
##
## SET TRUSTCERTS av_prca_pem_2033.txt,av_sipca_pem_2027.txt,av_csca_pem_2032.txt
## Note: The above is list of Avaya trusted certificates. You shall only use
## the ones that are required for your setup.
## Note: 96x1 H.323 R6.6 and later supports also intermediate certificates download for cases
## where servers do not provided the full certificate 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.
## Note: Avaya Vantage Basic application and Avaya Equinox uses the Android trusted certificate repository and the downloaded
certificates.
## using TRUSTCERTS.
##
## MAX_TRUSTCERTS specifies the maximum number of trusted
## certificate files, which are defined by TRUSTCERTS
## parameter, can be downloaded to the phone.

```

```
## Valid value: 1 to 10, default: 6
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0 and J100 SIP R2.0.0.0 and later
## 96x1 SIP 7.1.0.0 and later
## SET MAX_TRUSTCERTS 8
##
## ENABLE_PUBLIC_CA_CERTS specifies whether the embedded public root CA certificates are used for services other than Device
Enrollment Service (DES)
## and re-directed file server using DES. DES always used the embedded public root CA certificates (even if ENABLE_PUBLIC_CA_CERTS
is 0).
## For the re-directed file server using DES, there is use of embedded public root certificates if DES service did not provide private CA. If
DES provides private CA, then the
## embedded public root CA certificates are ignored (however if DES is re-triggered from admin menu and private CA is provided from
DES then the embedded public root CA certificates will be used according to ENABLE_PUBLIC_CA_CERTS).
## For rest of the services, this parameter controls whether embedded public root CA certificates are used (in addition, to downloaded
trusted certificates) or not (only downloaded trusted certificates are used).
## If DES did not provide private CA, then the ENABLE_PUBLIC_CA_CERTS is set to "1" without ability to change it. If DES provides
private CA, then this parameter is configurable (in such case, TRUSTCERTS shall include
## DES service private CA, else the phone will not be able to re-connect to the re-directed file server).
## For cases where DES is not used, then the parameter is fully configurable and if ENABLE_PUBLIC_CA_CERTS is "0" and no
downloaded trusted certificates (TRUSTCERTS=="") then the phone trusts for any HTTP/S file server
## for configuration / image download and fails with rest of services (PPM/SIP, AADS, etc). If either ENABLE_PUBLIC_CA_CERTS is "1"
and/or TRUSTCERTS<> "" then the service must have identity certificate that can be validated
## using the embedded public root CA certificates (if ENABLE_PUBLIC_CA_CERTS is "1") or downloaded trusted certificates (if
TRUSTCERTS<>"" ) - there is no exception to configuration and software files download from the HTTP/S file server
## in such case.
## Value Operation
## 0 Embedded public CA certs are not trusted (Default).
## 1 Embedded public CA certs are always trusted (in addition to trusted certificates downloaded according to TRUSTCERTS)
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.1.0.0 and later; the embedded public root CA certificates are Android public root certificates which
can be viewed in the settings application --> Security --> Trusted credentials --> SYSTEM.
## SET ENABLE_PUBLIC_CA_CERTS 1
## Note: This parameter is used on Avaya Vantage devices to enable all Android root CA certificates for non-Android applications such as
AADS, configuration and firmware download using HTTPS, PPM, 802.1x EAP-TLS, SCEP over HTTPS.
## This parameter cannot be used to disable Android root CA certificates for Android applications. CA_CERT_BLACKLIST shall be used
to disable Android root CA certificates for both Android and non-Android applications.
##
## TLSSRVRID specifies whether a certificate will be trusted only if the
## identity of the device from which it is received matches the certificate,
## per Section 3.1 of RFC 2818.
## Value Operation
## 0 Identity matching is not performed
## 1 Identity matching is performed (default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Equinox 3.1.2 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later; Not used by Avaya Vantage Open application.
## Avaya Vantage Basic Application SIP R1.0.0.0 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later; Supported by SIP/PPM and file downloads.
## B189 H.323 R1.0 and later
## 96x0 H.323 R2.0 and later
## 96x0 SIP R2.0 and later
## TLSSRVRID is not supported by 96x1 H.323 phones and instead
## TLSSRVRVERIFYID is supported (see below)
## SET TLSSRVRID 0
##

## FQDN_IP_MAP specifies a comma separated list of name/value pairs where the name is an FQDN and the value is an IP address.
## The IP address may be IPv6 or IPv4 but the value can only contain one IP address. Default is "". String length is up to 255
## characters. No spaces are allowed inside the string.
## The purpose of this parameter is to support cases where the server certificate Subject Common Name of Subject Alternative Names
## include FQDN (instead of IP address) and the SIP_CONTROLLER_LIST is defined using IP address. The main use case is for Avaya Aura
SM/PPM connectivity
## where the SIP controller list returned from Aura (PPM) to the endpoint is IP address only while server certificate is defined with
FQDN.
```

```

## Internet trusted CAs prefer signing of Internet public server certificates with FQDN only.
## This parameter is supported with any phone service running over TLS. Though, the main use case is for Avaya Aura SM/PPM services.
## This parameter is not to be used as an alternative to a DNS lookup or reverse DNS lookup.
## The reverse case will not be supported. If the phone is accessing a server using an FQDN and the server's certificate only contains an IP address,
## this will be considered a failure and the FQDN_IP_MAP will not be used.
## This parameter is supported by:
##   J100 SIP R2.0.0.0 and later
##   J129 SIP R1.0.0.0 (or R1.1.0.0) (IPv6 is not yet supported)
##   J169/J179 SIP R1.5.0
## SET FQDN_IP_MAP
"sm1.avaya.com=135.20.230.199,sm1.avaya.com=2000::204,sm2.avaya.com=135.20.230.201,ppm.ottawa.avaya.com=2000::207"
##
## SERVER_CERT_RECHECK_HOURS 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.
## SERVER_CERT_RECHECK_HOURS is applicable for H.323 over TLS signaling only in 96x1 H.323 R6.6.
## SERVER_CERT_RECHECK_HOURS is applicable for SIP and 802.1x EAP-TLS when used by J129 SIP R1.0.0.0 and later.
## Valid values are: 0-32767. A value of 0 means that periodic checks will not be done.
## The default is 24.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   96x1 SIP R7.1.0.0 and later
##   96x1 H.323 R6.6 and later
## SET SERVER_CERT_RECHECK_HOURS 30
##
## CERT_WARNING_DAYS specifies how many days before the expiration of a certificate that a warning
## should first appear on the phone screen. This includes trusted certificates, OCSP certificates and identity certificate.
## Log and syslog message will be generated as well. The warning will reappear every 7 days.
## Valid values are: 0-99 (60 is default), where 0 means no certificate expiration warning will be generated.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   96x1 SIP R7.1.0.0 and later
##   Avaya Vantage Devices SIP R1.0.0.0 and later
##   96x1 H.323 R6.6 and later
## SET CERT_WARNING_DAYS 30
##
## DELETE_MY_CERT specifies whether the installed identity certificate (using SCEP or PKCS12 file download) will be deleted.
## Value Operation
## 0 Installed Identity certificate remain valid (Default)
## 1 Installed Identity certificate is removed.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   96x1 SIP R7.1.0.0 and later
##   Avaya Vantage Devices SIP R1.0.0.0 and later
## SET DELETE_MY_CERT 1
##

##### TLS SETTINGS #####
##

##
## TLS_VERSION controls TLS version used for all TLS connections (except SLA monitor agent)
## Value Operation
## 0 TLS versions 1.0 and 1.2 are supported (default).
## 1 TLS version 1.2 only is permitted.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   Avaya Vantage Devices SIP R1.0.0.0 and later; Not used by Avaya Vantage Open application.
##   96x1 SIP R7.0.1.0 and later releases
##   96x1 H.323 R6.6.2 and later releases
##   B189 H.323 R6.6.2 and later releases
## SET TLS_VERSION 1
##

##### HTTP PROXY SERVER SETTINGS #####
##
## HTTPPROXY specifies the address of the HTTP proxy server used by SIP
## telephones to access an SCEP server that is not on the enterprise network.

```



```

## Zero or one IP address in dotted decimal or DNS name format,
## optionally followed by a colon and a TCP port number.
## The value can contain 0 to 255 characters; the default value is null ("").
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   Avaya Vantage Devices SIP R1.0.0.0 and later; HTTPPROXY is NOT supported for SCEP, but for Android HTTP based applications.
##   96x1 SIP R6.0 and later
##   H1xx SIP R1.0 and later; HTTPPROXY is NOT supported for SCEP, but for WEB Browser and Exchange.
##   96x0 SIP R1.0 and later
## Note that in H.323 telephones, SCEP uses WMLPROXY.
## SET HTTPPROXY proxy.mycompany.com
##
## HTTPEXCEPTIONDOMAINS specifies a list of one or more domains,
## separated by commas without any intervening spaces,
## for which HTTPPROXY will not be used.
## The value can contain 0 to 255 characters; the default value is null ("").
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   Avaya Vantage Devices SIP R1.0.0.0 and later; HTTPPROXY is NOT supported for SCEP, but for Android HTTP based applications.
##   96x1 SIP R6.0 and later
##   H1xx SIP R1.0 and later; HTTPEXCEPTIONDOMAINS is NOT supported for SCEP, but for WEB Browser and Exchange.
##   96x0 SIP R1.0 and later
## Note that in H.323 telephones, SCEP uses WMLEXCEPT.
## SET HTTPEXCEPTIONDOMAINS mycompany.com

##### SCEP SETTINGS #####
##
## Note: When FIPS_ENABLED is set to 1 (for endpoints which support FIPS mode), SCEP shall not be used.
## If identity certificate was generated before FIPS_ENABLED is set to 1, the phone will keep using it.
## However, it is NOT recommended to use identity certificate generated using SCEP when FIPS_ENABLED is 0 when
## the phone is configured to work in FIPS mode (FIPS_ENABLED==1). It is recommended to CLEAR (return to factory defaults)
## before configuring the phone to FIPS mode (FIPS_ENABLED==1).
##
## MYCERTURL specifies the URL of the SCEP server from which
## the telephone should obtain an identity certificate,
## if it does not already have one from that server.
## Zero to 255 ASCII characters; the default value is null ("").
## This parameter is supported by:
##   J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later - the URL can be https or http.
##   Avaya Vantage Devices SIP R1.0.0.0 and later; the URL can be https or http. Avaya Vantage Open application does not use identity
##   certificate.
##   96x1 H.323 R6.0 and later
##   H1xx SIP R1.0 and later
##   B189 H.323 R6.6 and later
##   96x1 SIP R6.0 up to R7.1.0.0 (excluded) - the URL can be only http; R7.1.0.0 and later - the URL can be https or http.
##   96x0 H.323 R3.1 and later
##   96x0 SIP R1.0 and later
## SET MYCERTURL http://certsrvr.trustus.com/mscep/mscep.dll
## SET MYCERTURL https://10.10.10.10/certsrv/mscep/mscep.dll
##
## MYCERTCN specifies the Common Name (CN) used in the SUBJECT of an SCEP
## certificate request. 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, including spaces.
## Eight (" $MACADDR") to 255 characters; the default value is "$SERIALNO".
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   Avaya Vantage Devices SIP R1.0.0.0 and later; Avaya Vantage Open application does not use identity certificate.
##   96x1 H.323 R6.0 and later
##   B189 H.323 R6.6 and later
##   96x1 SIP R6.0 and later
##   H1xx SIP R1.0 and later
##   96x0 H.323 R3.1 and later
##   96x0 SIP R1.0 and later
## Note that prior to R2.6.8, 96x0 SIP releases only support
## "$MACADDR" or "$SERIALNO" as a value, not additional characters.
## SET MYCERTCN "Avaya telephone with MAC address $MACADDR"

```

```

##
## MYCERTDN specifies the part the SUBJECT of an SCEP certificate request
## that is common for all telephones. It must begin with a "/" and may
## include Organizational Unit, Organization, Location, State and Country.
## Zero to 255 ASCII characters; the default value is null ("").
## Note: It is recommended that "/" be used as a separator between components.
## Commas have been found to not work with some servers.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later; Avaya Vantage Open application does not use identity certificate.
## 96x1 H.323 R6.0 and later
## B189 H.323 R6.6 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 H.323 R3.1 and later
## 96x0 SIP R1.0 and later
## SET MYCERTDN /C=US/ST=NJ/L=MyTown/O=MyCompany
##
## MYCERTCAID specifies an identifier for the CA certificate with which
## the SCEP certificate request is to be signed, if the server hosts
## multiple Certificate Authorities.
## Zero to 255 ASCII characters; the default value is "CAIdentifier".
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later; Avaya Vantage Open application does not use identity certificate.
## 96x1 H.323 R6.0 and later
## B189 H.323 R6.6 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 H.323 R3.1 and later
## 96x0 SIP R1.0 and later
## SET MYCERTCAID EjbSubCA
##
## MYCERTKEYLEN specifies the bit length of the public and private keys
## generated for the SCEP certificate request.
## 4 ASCII numeric digits, "1024" through "2048"; the default value is "1024".
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later; only "2048" is supported
## Avaya Vantage Devices SIP R1.0.0.0 and later; only value "2048" is supported.
## 96x1 H.323 R6.0 and later
## B189 H.323 R6.6 and later
## 96x1 SIP R6.0 and later; default value is "2048" in 96x1 SIP R6.5+. 96x1 SIP R7.1.0.0 and later - only "2048" is supported.
## H1xx SIP R1.0 and later; default value is "2048" in H1xx SIP R1.0.1+.
## 96x0 H.323 R3.1 and later
## 96x0 SIP R1.0 and later
## SET MYCERTKEYLEN 1024
##
## MYCERTRENEW specifies the percentage of the identity certificate's
## Validity interval after which renewal procedures will be initiated.
## Valid values are 1 through 99; the default value is 90.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 H.323 R6.0 and later
## B189 H.323 R6.6 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 H.323 R3.1 and later
## 96x0 SIP R1.0 and later
## SET MYCERTRENEW 90
##
## MYCERTWAIT specifies the telephone's behavior if the SCEP server
## indicates that the certificate request is pending manual approval.
## Value Operation
## 0 Poll the SCEP server periodically in the background
## 1 Wait until a certificate is received or the request is rejected (default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later

```



```

## 96x1 H.323 R6.0 and later
## B189 H.323 R6.6 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 H.323 R3.1 and later
## 96x0 SIP R1.0 and later
## SET MYCERTWAIT 1
##
## SCEPPASSWORD specifies the password to be included (if not null)
## in the challengePassword attribute of an SCEP certificate request.
## Values may contain 0 to 32 ASCII characters (50 ASCII characters in 96x1/B189 H.323 6.6 and later);
## the default value is "$SERIALNO".
## If the value contains "$SERIALNO", it will be replaced by the telephone's serial number.
## If the value contains "$MACADDR", it will be replaced by the telephone's MAC address in hex.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later; please note that if SCEP is configured and SCEPPASSWORD is empty,
## the user will be prompted to enter the SCEP password.
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later; please note that if SCEP is configured and SCEPPASSWORD is empty,
## the user will be prompted to enter the SCEP password. Avaya Vantage Open application does not use
identity certificate.
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.2 and later
## H1xx SIP R1.0 and later
## 96x0 H.323 R3.1 and later
## B189 H.323 R6.6 and later
## Note that to maintain the security of the password, this parameter should
## not be set in a file that is accessible on an enterprise network,
## it should only be set in a restricted staging configuration.
## SET SCEPPASSWORD $SERIALNO
##

##### PKCS12 SETTINGS #####
##
## PKCS12URL specifies the URL to be used to download a PKCS #12 file
## containing an identity certificate and its private key.
## 0 to 255 ASCII characters, zero or one URL. The value can 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.
## If $MACADDR is added to the URL then the PKCS12 filename on the file server shall include MAC address
## without colons (i.e., 6 pairs of ASCII hexadecimal characters AABCCDDDEEFF with hex characters A-F
## encoded as upper-case characters). For example, if Ethernet MAC address of a specific phone
## is: 00-24-D7-E4-2E-98 and the PKCS12URL is: http://pkc12file_$MACADDR.cer, then the filename of the
## PKCS12 file for this phone on the file server shall be: pkc12file_0024D7E42E98.cer.
## PKCS12 file download is preferred over SCEP if PKCS12URL is defined.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later
## J169/J179 SIP R1.5.0; Same note as for 96x1 SIP R7.1.0.0 below.
## 96x1 SIP R7.1.0.0 and later; The URL can specify the file server using an IPv4/IPv6 address or an FQDN.
## An empty parameter value means that PKCS#12 identity certificate download is disabled (if there is
## an already existing PKCS12 file on the phone then it will not be deleted if PKCS12URL is set to "").
## DELETE_MY_CERT shall be set to 1 or CLEAR procedure shall be used to delete existing PKCS12 file).
## If the parameter is not empty, PKCS#12 file installation is preferred over SCEP.
## Avaya Vantage Devices SIP R1.0.0.0 (build 2304) and later; Avaya Vantage Open application does not use identity certificate.
## 96x1 H.323 R6.6 and later
## SET PKCS12URL http://pkc12file_$MACADDR.cer
##
## PKCS12_PASSWD_RETRY specifies the number of retries for entering PKCS12 file password.
## Values: 0-100 and the default is 3. 0 means no retry.
## If user failed to enter the correct PKCS12 file password after PKCS12_PASSWD_RETRY retries, then the
## phone will continue the startup sequence without installation of PKCS12 file.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later## Avaya Vantage Devices SIP R1.0.0.0 (build 2304) and later; Avaya Vantage Open application does
not use identity certificate.
## SET PKCS12_PASSWD_RETRY 4
##

```

```
##### 802.1X SETTINGS #####
##
## DOT1XSTAT specifies the 802.1X Supplicant operating mode.
## Value Operation
## 0 Supplicant disabled (default, unless indicated otherwise below)
## 1 Supplicant enabled, but responds only to received unicast EAPOL messages
## 2 Supplicant enabled; responds to received unicast and multicast EAPOL messages
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later

## H1xx SIP R1.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## B189 H.323 R1.0 and later
## 96x0 H.323 R2.0 and later
## 96x0 SIP R2.0 and later (default was 1 prior to R2.4.1)
## SET DOT1XSTAT 1
##
## DOT1X specifies the 802.1X pass-through operating mode.
## Pass-through is the forwarding of EAPOL frames between the telephone's
## Ethernet line interface and its secondary (PC) Ethernet interface
## Value Operation
## 0 EAPOL multicast pass-through enabled without proxy logoff (default)
## 1 EAPOL multicast pass-through enabled with proxy logoff
## 2 EAPOL multicast pass-through disabled
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.1.0.0 and later for K165/K175 models with embedded Ethernet switch
## H1xx SIP R1.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## 96x0 H.323 R2.0 and later
## 96x0 SIP R2.0 and later
## Note: In 96x0 H.323 releases 1.0 through 1.5, DOT1X is supported, but it controls both Supplicant and pass-through operation.
## In these releases, operation is as follows:
## Value Operation
## 0 Unicast Supplicant and multicast pass-through enabled without proxy logoff (default)
## 1 Unicast Supplicant and multicast pass-through enabled with proxy logoff
## 2 Unicast or multicast Supplicant operation enabled, without pass-through
## SET DOT1X 1
##
## DOT1XEAPS specifies the authentication method to be used by 802.1X.
## Valid values are "MD5" (the default) and "TLS".
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later
## H1xx SIP R1.0 and later
## 96x1 H.323 R6.2.1 and later
## 96x1 SIP R6.0 and later
## 96x0 H.323 R3.1.4 and later
## 96x0 SIP R2.0 and later
## B189 H.323 R6.6 and later
## SET DOT1XEAPS MD5
##

##### FIPS SETTINGS #####
##
## FIPS_ENABLED specifies whether only FIPS-approved cryptographic algorithms will be supported.
## Value Operation
## 0 No restriction on using non FIPS-approved cryptographic algorithms (default)
## 1 Use only FIPS-approved cryptographic algorithms using embedded FIPS 140-2-validated cryptographic module (Per NIST
Certificate #1747,
## for the exact operational environment used by the endpoint please refer to the Avaya support team).
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later
## 96x1 SIP 7.1.0.0 and later
```

```

## 96x1 H.323 R6.6 and later
## SET FIPS_ENABLED 1
##
##### OCSP (Online Certificate Status Protocol) SETTINGS #####
##
## OCSP_ENABLED specifies whether OCSP will be used to check revocation status of certificates.
## Value Operation
## 0 OCSP is disabled (default)
## 1 OCSP is enabled. OCSP will be used to check revocation status for the certificates
## presented by peers for any TLS connection (H.323 signaling over TLS, HTTPS,
## 802.1x with EAP-TLS, SLA Mon agent, IPSec VPN, SSO)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## 96x1 H.323 R6.6 and later
## SET OCSP_ENABLED 1
##
## OCSP_ACCEPT_UNK specifies whether in cases where certificate revocation status for a specific certificate
## cannot be determined to bypass certificate revocation operation for this certificate.
## Value Operation
## 0 Certificate is considered to be revoked if the certificate revocation status is unknown. TLS connection
## will be closed.
## 1 Certificate revocation operation will accept certificates for which the certificate revocation
## status is unknown (default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## 96x1 H.323 R6.6 and later
## SET OCSP_ACCEPT_UNK 1
##
## OCSP_NONCE specifies whether a nonce will be included in OCSP requests and expected in OCSP responses.
## Value Operation
## 0 Nonce is NOT added to OCSP packets
## 1 Nonce is added to OCSP packets (Default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## 96x1 H.323 R6.6 and later
## SET OCSP_NONCE 1
##
## OCSP_URI specifies the URI of an OCSP responder. The URI can be an IP address or hostname.
## The default is "". 0 to 255 ASCII characters - zero or one URI.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## 96x1 H.323 R6.6 and later
## SET OCSP_URI http://clients1.google.com/ocsp
##
## OCSP_URI_PREF specifies the preferred URI to use for OCSP requests if more than one is available.
## Value Operation
## 1 Use the OCSP_URI first and then the OCSP field of the Authority Information Access (AIA) extension
## of the certificate being checked (Default)
## 2 Use the OCSP field of the Authority Information Access (AIA) extension of the
## certificate being checked first and then OCSP_URI
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## 96x1 H.323 R6.6 and later
## SET OCSP_URI_PREF 0
##
## OCSP_TRUSTCERTS 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.
## 0 to 255 ASCII characters: zero or more file names or URLs, separated by commas without any intervening spaces
## The default is "".
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later

```

```

## 96x1 SIP R7.1.0.0 and later
## 96x1 H.323 R6.6 and later
## SET OCSP_TRUSTCERTS ocsf.cer
##
## OCSP_HASH_ALGORITHM specifies the hashing algorithm for OCSP request.
## Value Operation
## 0 SHA-1 (default)
## 1 SHA-256
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## SET OCSP_HASH_ALGORITHM 1
##
## OCSP_USE_CACHE specifies if OCSP caching is used.
## Value Operation
## 0 Do not to use OCSP caching. Always check with OCSP responder.
## 1 Use OCSP cache caching (default).
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## SET OCSP_USE_CACHE 1
##
## OCSP_CACHE_EXPIRY specifies the cache expiry in minutes.
## Valid values: 60 to 10080 (60 min to 7 days) with default 2880 (2 days).
## Note that OCSP response cache expiry uses nextUpdate value in OCSP response message. Only if nextUpdate is not present will the
OCSP_CACHE_EXPIRY parameter value be used.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## SET OCSP_CACHE_EXPIRY 1
##

##### IDLE TIMER SETTINGS #####
##
## BAKLIGHTOFF specifies the number of minutes of idle time after which the display backlight will be turned off.
## Phones with gray-scale displays do not completely turn backlight off, they set it to the lowest non-off level.
## Valid values are 0 through 999; the default value is 120 (2 hours).
## A value of 0 means that the display backlight will not be turned off automatically when the phone is idle.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## Avaya Vantage Devices SIP R1.0.0.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.2 and later
## B189 H.323 R1.0 and later
## H1xx SIP R1.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## SET BAKLIGHTOFF 60
##

##
## SCREENSAVERON specifies the number of minutes of idle time after which the screen saver will be displayed.
## If an image file has been downloaded based on the SCREENSAVER (H.323), LOGOS and CURRENT_LOGO
## (for 96x0 R1.0 SIP and later, 96x1 R6.0 SIP and later and J169/J179 SIP R1.5.0) or SCREENSAVER_IMAGE
## (for J100 SIP R2.0 and later) parameters, it will be used as the screen saver.
## Otherwise, the built-in Avaya one-X(TM) screen saver will be used.
## Valid values are 0 through 999; the default value is 240 (4 hours).
## A value of 0 means that the screen saver will not be displayed automatically when the phone is idle.
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later (J169 and J179 only)
## J169/J179 SIP R1.5.0
## 96x1 SIP R6.0 and later
## B189 H.323 R1.0 and later
## 96x0 H.323 R1.0 and later, but not supported by the 9610
## 96x0 SIP R1.0 and later
## SET SCREENSAVERON 480
##

```

```
##### PHONE LOCK SETTINGS (SIP ONLY) #####
##
## ENABLE_PHONE_LOCK specifies whether a softkey (on the idle Phone screen) and
## a feature button will be displayed to allow the user to manually lock the phone.
## Value Operation
## 0 Disabled: Lock softkey and feature button will not be displayed (default)
## 1 Enabled: Lock softkey and feature button will be displayed
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later; Please note that on J129 the Lock option appears
## in the main menu. There is no Lock softkey or feature button.
## Avaya Vantage Devices SIP R1.0.0.0 and later; Please note that ENABLE_PHONE_LOCK is used as enable/disable
## of lock screen.
## 96x1 SIP R6.0 and later
## 96x0 SIP R2.5 and later
## H1xx SIP R1.0 and later; Please note that ENABLE_PHONE_LOCK is used on H1xx as enable/disable
## of lock screen.
## SET ENABLE_PHONE_LOCK 1
##
## PHONE_LOCK_IDLETIME specifies the interval of idle time, in minutes, after which
## the phone will automatically lock if the value of ENABLE_PHONE_LOCK is 1.
## A value of 0 means that the phone will not lock automatically.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later; valid values are 0 through 10080; the default value is 0. The parameter
is supported
## no matter what is the ENABLE_PHONE_LOCK value is.
## J169/J179 SIP R1.5.0; valid values are 0 through 10080; the default value is 0.
## Avaya Vantage Devices SIP R1.0.0.0 and later; valid values are 1 through 10080; the default value is 60. Please note
PHONE_LOCK_IDLETIME
## specifies the maximum interval of idle time, in minutes, allowed for user configuration (unless exchange policy enforces lower
number).
## User can choose smaller value than this value in the settings application. By default, user choice is 5 minutes.
## 96x1 SIP R6.2 and later; valid values are 0 through 10080; the default value is 0.
## 96x1 SIP R6.0.x; valid values are 0 through 999; the default value is 0.
## 96x0 SIP R2.5 and later; valid values are 0 through 999; the default value is 0.
## H1xx SIP R1.0 and later; valid values are 1 through 10080; the default value is 60. Please note PHONE_LOCK_IDLETIME
## specifies the maximum interval of idle time, in minutes, allowed for user configuration (unless exchange policy enforces lower
number).
## User can choose smaller value than this value in the settings application. By default, user choice is 5 minutes.
## SET PHONE_LOCK_IDLETIME 30
##

##### CODEC AND RTP SETTINGS (SIP ONLY) #####
##
## ENABLE_G711A specifies whether the G.711 a-law codec is enabled.
## Value Operation
## 0 Disabled
## 1 Enabled (default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## 96x0 SIP R1.0 and later
## H1xx SIP R1.0 and later
## SET ENABLE_G711A 0
##
## ENABLE_G711U specifies whether the G.711 mu-law codec is enabled.
## Value Operation
## 0 Disabled
## 1 Enabled (default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## 96x0 SIP R1.0 and later
## H1xx SIP R1.0 and later
## SET ENABLE_G711U 0
##
## ENABLE_G722 specifies whether the G.722 codec is enabled.
## Value Operation
## 0 Disabled
```

```

## 1 Enabled
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later; the default value is 1.
## 96x1 SIP R6.2 and later; the default value is 1.
## 96x1 SIP R6.0.x; the default value is 0.
## 96x0 SIP R2.0 and later; the default value is 0.
## H1xx SIP R1.0 and later; the default value is 1.
## SET ENABLE_G722 1
##
## ENABLE_G726 specifies whether the G.726 codec is enabled.
## Value Operation
## 0 Disabled (default for 96x0 R1.0)
## 1 Enabled (default for all other releases and models)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## 96x0 SIP R1.0 and later
## H1xx SIP R1.0 and later; For IP office environment this parameter shall be set to 0 as G.726 is not supported by IP Office.
## SET ENABLE_G726 0
##
## G726_PAYLOAD_TYPE specifies the RTP payload type to be used for the G.726 codec.
## Valid values are 96 through 127; the default value is 110.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R1.0 and later
## SET G726_PAYLOAD_TYPE 111
##
## ENABLE_G729 specifies whether the G.729A codec is enabled.
## Value Operation
## 0 Disabled
## 1 Enabled without Annex B support (default)
## 2 Enabled with Annex B support
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## 96x0 SIP R1.0 and later
## H1xx SIP R1.0 and later
## SET ENABLE_G729 0
##
## ENABLE_OPUS specifies whether the OPUS codec is enabled.
## Value Operation
## 0 Disabled
## 1 Enabled WIDEBAND_20K (default value).
## 2 Enabled NARROWBAND_16K
## 3 Enabled NARROWBAND_12K
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later; for IP office and 3PCC environments this
## parameter shall be set to 0 (As OPUS is supported in Avaya Aura environment only).
## Avaya Equinox 3.1.2 and later
## Avaya Vantage Basic Application SIP R1.0.0.1 and later; supported in both Aura and IPO environments.
## SET ENABLE_OPUS 0
##
## OPUS_PAYLOAD_TYPE specifies the RTP payload type to be used for the OPUS codec.
## Valid values are 96 through 127; the default value is 116.
## This parameter is used when media offer is sent to the far end
## in an INVITE (or 200 OK when INVITE with no SDP is received).
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later
## Avaya Equinox 3.1.2 and later
## Avaya Vantage Basic Application SIP R1.0.0.1 and later
## SET OPUS_PAYLOAD_TYPE 111
##
## SEND_DTMF_TYPE specifies whether DTMF tones are sent in-band (as regular audio),
## or out-of-band (using RFC 2833 procedures).
## Value Operation
## 1 in-band

```

```

## 2 out-of-band (default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0 and later
## 96x0 SIP R1.0 and later
## H1xx SIP R1.0 and later
## SET SEND_DTMF_TYPE 1
##
## DTMF_PAYLOAD_TYPE specifies the RTP payload type to be used for RFC 2833 signaling.
## Valid values are 96 through 127; the default value is 120.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Equinox 3.1.2 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R1.0 and later
## SET DTMF_PAYLOAD_TYPE 121
##
## SYMMETRIC_RTP specifies whether or not the telephone should discard
## received RTP/SRTP datagrams if their UDP Source Port number is not
## the same as the UDP Destination Port number that the telephone is
## including in RTP/SRTP datagrams intended for that endpoint.
## Value Operation
## 0 Ignore the UDP Source Port number in received RTP/SRTP datagrams.
## 1 Discard received RTP/SRTP datagrams if their UDP Source Port number
## does not match the UDP Destination Port number that the telephone is
## including in RTP/SRTP datagrams intended for that endpoint (default).
## This parameter is supported by:
## J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.1.0 and later (9608 and SIP9611 HW version 3 and higher)
## 96x1 SIP R6.0 and later (hardware version below 3).
## H1xx SIP R1.0 and later
## 96x0 SIP R2.4 and later
## SET SYMMETRIC_RTP 0
##

##### OTHER SIP-ONLY SETTINGS #####
##
## PHNMUTEALERT_BLOCK specifies whether the Mute Alert feature will be Blocked or Unblocked.
## Value Operation
## 0 Unblocked
## 1 Blocked (default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.0.1 and later.
## SET PHNMUTEALERT_BLOCK 1
##
## MATCHTYPE specifies how a calling party number is compared to the numbers
## in the user's Contacts to obtain a name to display for the incoming call.
## Value Operation (for 96x1 SIP R6.2 to R7.0 (excluded), 96x0 R2.6.5 and later)
## 0 The Contact name is displayed if the rightmost 4 digits of the calling
## party number match the rightmost 4 digits of a Contacts number (default)
## 1 The Contact name is displayed if the entire calling party number
## exactly matches the all of the digits in a Contacts number
## Value Operation (for 96x1 SIP R7.0 and later)
## 0 The Contact name is displayed if the entire calling/called party number exactly matches
## the number stored in the contact (ELD rules are applied) (default)
## 1 The Contact name is displayed if all the digits of the shorter number (contacts, calling/called party number)
## match to the rightmost digits of the longer number (contacts, calling/called party number).
## 2 The Contact name is displayed if at least 4 rightmost digits of the calling/called
## party number match the rightmost 4 digits of a Contacts number
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R6.2 and later
## 96x0 SIP R2.6.5 and later.
## SET MATCHTYPE 0
##

```



```

##
##### SIG SETTING #####
##
## SIG specifies the type of software to be used by the telephone by
## controlling which upgrade file is requested after a power-up or a reset.
## Value Operation
## 0 Download the upgrade file for the same signaling protocol
## that is supported by the current software (default)
## 1 Download 96x1Hupgrade.txt (for H.323 software)
## 2 Download 96x1Supgrade.txt (for SIP software)
## This parameter is supported by:
## J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## SET SIG 0
##
##### ETHERNET INTERFACE SETTINGS #####
##
## PHY1STAT specifies the speed and duplex settings for the Ethernet line interface.
## Valid values are 1 through 6; the default value is 1.
## Value Operation
## 1 auto-negotiate
## 2 10Mbps half-duplex
## 3 10Mbps full-duplex
## 4 100Mbps half-duplex
## 5 100Mbps full-duplex
## 6 1Gbps full-duplex if supported by hardware, otherwise auto-negotiate
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later (values 1-5 only)
## H1xx SIP R1.0 and later (values 1-5 only)
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.2 and later (values 1-5 only)
## B189 H.323 R1.0 and later
## 96x1 SIP R6.0.x
## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## SET PHY1STAT 1
## Note: The parameter is permanently configured to "Auto-Negotiate" on Avaya Vantage SIP R1.1.0.0 and later.
##
## PHY2STAT specifies the speed and duplex settings for the secondary (PC) Ethernet interface.
## Valid values are 0 through 6; the default value is 1.
## Value Operation
## 0 disabled
## 1 auto-negotiate
## 2 10Mbps half-duplex
## 3 10Mbps full-duplex
## 4 100Mbps half-duplex
## 5 100Mbps full-duplex
## 6 1Gbps full-duplex if supported by hardware, otherwise auto-negotiate
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later (values 0-5 only)
## Avaya Vantage Devices SIP R1.1.0.0 and later for K165/K175 models with embedded Ethernet switch (values 0-1 only)
## H1xx SIP R1.0 and later (values 0-5 only)
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.2 and later (values 0-5 only)
## 96x1 SIP R6.0.x
## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## SET PHY2STAT 1
##
## PHY2_AUTOMDIX_ENABLED specifies whether auto-MDIX is enabled on PHY2.
## Valid values are 0 through 1; the default value is 1.
## Value Operation
## 0 auto-MDIX is disabled
## 1 auto-MDIX is enabled (default).
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.1.0.0 and later for K165/K175 models with embedded Ethernet switch

```



```

## H1xx SIP R1.0 and later
## 96x1 H.323 R6.3 and later
## 96x1 SIP R6.3 and later
## SET PHY2_AUTOMDIX_ENABLED 1
##
##
## EEESTAT controls whether Energy-Efficient Ethernet (802.3az) is enabled on PHY1 and PHY2.
## Value Operation
## 0 EEE is disabled
## 1 EEE is enabled (default).
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later (J129 only)
## SET EEESTAT 0

##### LOCAL PROCEDURE ACCESS SETTINGS #####
##
## PROCSTAT specifies whether local (craft) procedures can be used to configure the telephone.
## Value Operation
## 0 Local procedures can be used (default)
## 1 Local procedures cannot be used
## Note: Be very careful before setting PROCSTAT to 1
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## B189 H.323 R1.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## SET PROCSTAT 1
##
## PROCPSWD specifies an access code for access to local (craft) procedures.
## Valid values contain 0 through 7 ASCII numeric digits.
## The default value is 27238 (CRAFT) unless indicated otherwise below.
## A null value implies that an access code is not required for access.
## Note: Setting this parameter via CM (for H.323) or PPM (for SIP) is more secure
## because this file can usually be accessed and read by anyone on the network.
## Setting the value in this file is intended primarily for configurations with
## versions of telephone or server software that do not support setting this
## value from the server.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later (must contain at least 4 digits
## else default value 27238 is used)
## Avaya Vantage Devices SIP R1.0.0.0 and later (must contain at least 4 digits)
## 96x1 H.323 R6.0 and later (must contain at least 4 digits for R6.2.4 and later,
## else default value 27238 is used)
## 96x1 SIP R6.0 and later (must contain at least 4 digits for R6.3 and later
## else default value 27238 is used)
## H1xx SIP R1.0 and later (must contain at least 4 digits else default value
## 27238 is used)
## B189 H.323 R1.0 and later (must contain at least 4 digits for R1.0 and later
## else default value 27238 is used)
## 96x0 H.323 R1.0 and later (default is null ("") prior to R1.2, must contain at
## least 4 digits for R3.2.1 and later else default value
## 27238 is used)
## 96x0 SIP R1.0 and later (must contain at least 4 digits for R2.6.10 and later
## else default value 27238 is used)
## SET PROCPSWD 572958
##
## ADMIN_PASSWORD specifies a complex access code for access to local (craft) procedures.
## Valid values contain 6 and 31 alphanumeric characters including upper, lower and special characters.
## The default value is 27238 which implies that PROCPSWD is used as access code for access to local (craft) procedures.
## If ADMIN_PASSWORD length is less than 6 or greater than 31, the parameter is treated as not defined.
## If ADMIN_PASSWORD is configured, then PROCPSWD is ignored.
## The special characters supported are: ~!@#%&*_-+=\|{}[]:;<>.,?/. " is not supported.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 (build 2304) and later; the default value is "". ADMIN_PASSWORD is not applied on Boot
## Recovery Menu (BRM).

```

```

## 96x1 SIP R7.1.0.0 and later
## Avaya Vantage Basic Application SIP R1.0.0.0 and later; default value is "".
## Note: For Avaya Vantage Basic Application and Avaya Vantage Devices, if ADMIN_PASSWORD is not configured and PROCPSWD is not
configured, then the
## local (craft) procedures are not accessible.
## Note: The parameter is also used by "Avaya Vantage Basic Application" to allow administrator
## to unpin/pin the application when PIN_APP is defined to "Avaya Vantage Basic Application" package name.
## SET ADMIN_PASSWORD ComPlexPSWD12?!
##
## ADMIN_LOGIN_ATTEMPT_ALLOWED specifies the number of failed attempts for entering the access code (PROCPSWD or
ADMIN_PASSWORD)
## before the local (craft) procedures will be locked for a period specified by ADMIN_LOGIN_LOCKED_TIME.
## Valid values are 1 to 20, default 10.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## SET ADMIN_LOGIN_ATTEMPT_ALLOWED 11
##

```

```

##### SNMP SETTINGS #####
##
## SNMPSTRING specifies a security string that must be included in SNMP query messages
## for the query to be processed.
## Valid values contain 0 through 32 ASCII alphanumeric characters.
## The default value is null ("") unless indicated otherwise below.
## A null value results in SNMP being disabled.
## Note: Setting this parameter via CM (for H.323) or PPM (for SIP) is more secure
## because this file can usually be accessed and read by anyone on the network.
## Setting the value in this file is intended primarily for configurations with
## older versions of telephone, CM or PPM software that do not support setting
## this value from the server.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## B189 H.323 R1.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## SET SNMPSTRING mystring
##
## SNMPADD specifies a list of source IP addresses from which SNMP query messages
## will be accepted and processed.
## Addresses can be in dotted-decimal (IPv4), colon-hex (IPv6, if supported), or
## DNS name format, separated by commas without any intervening spaces.
## The list can contain up to 255 characters; the default value is null ("").
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## B189 H.323 R1.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## SET SNMPADD 192.168.0.22,192.168.0.23
##
##### LINK LAYER DISCOVERY PROTOCOL (LLDP) SETTINGS #####
##
## LLDP_ENABLED specifies whether LLDP is enabled.
## Value Operation
## 0 Disabled
## 1 Enabled
## 2 Enabled, but only begin transmitting if an LLDP frame is received (default)
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later; the default is 1.
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later; the default is 1.
## 96x0 SIP R2.0 and later

```

```

## Note that the following do NOT support the LLDP_ENABLED parameter,
## but they always operate consistent with a value of 2 above:
##   96x1 H.323 R6.0 and later
##   B189 H.323 R1.0 and later
##   96x0 H.323 R1.2 and later
## SET LLDP_ENABLED 1

##### EVENT LOGGING SETTINGS #####
##

## LOGSRVR specifies one address for a syslog server
## in dotted-decimal (IPv4), colon-hex (IPv6, if supported), or DNS name format.
## The value can contain 0 to 255 characters; the default value is null ("").
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   Avaya Vantage Devices SIP R1.0.0.0 and later
##   96x0 H.323 R1.0 and later
##   96x0 SIP R1.0 and later
##   96x1 H.323 R6.0 and later
##   96x1 SIP R6.0 and later
##   B189 H.323 R1.0 and later
##   H1xx SIP R1.0 and later
## SET LOGSRVR 192.168.0.15
##

## LOCAL_LOG_LEVEL specifies the severity levels of events logged in the
## endptRecentLog, endptResetLog and endptStartupLog objects in the SNMP MIB.
## Events with the selected severity level and above will be logged
## (note that lower numeric severity values correspond to higher severity levels).
## Value Operation
## 0 Emergency events are logged
## 1 Alert and Emergency events are logged
## 2 Critical, Alert and Emergency events are logged
## 3 Error, Critical, Alert and Emergency events are logged (default)
## 4 Warning, Error, Critical, Alert and Emergency events are logged
## 5 Notice, Warning, Error, Critical, Alert and Emergency events are logged
## 6 Informational, Notice, Warning, Error, Critical, Alert and Emergency events are logged
## 7 Debug, Informational, Notice, Warning, Error, Critical, Alert and Emergency events are logged
## Warning: A setting of 7 can impact the performance of the telephone due to the number of events generated.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or 1.1.0.0), J169/J179 SIP R1.5.0 and J100 SIP R2.0.0.0 and later
##   Avaya Vantage Devices SIP R1.0.0.0 and later; No SNMP support in R1.0.0.0. This parameter affects local log files stored on the
device.
##   96x0 SIP R1.0 and later
##   96x1 SIP R6.0 and later
##   H1xx SIP R1.0 and later; No SNMP support in R1.0. This parameter affects local log files stored on the device.
## SET LOCAL_LOG_LEVEL 3
##

## LOG_CATEGORY specifies a list of categories of events to be logged via syslog and locally.
## This parameter must be specified to log events below the Error level.
## The list can contain up to 255 characters. The default is "".
## Category names are separated by commas without any intervening spaces.
## See Administrator's guide for additional detail.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   Avaya Vantage Devices SIP R1.0.0.0 and later; the default is "ALL" which implies all categories.
##   96x0 SIP R1.0 and later
##   96x1 SIP R6.0 and later
##   H1xx SIP R1.0 and later; the default is "ALL" which implies all categories. New categories for H1xx compare to
##   96x1 SIP: "ANDROID" and "KERNEL".
## SET LOG_CATEGORY DHCP,NETMGR,AUDIO
##

##### AUDIO DEBUG RECORDING #####
##

## ENABLE_RECORDING specifies whether audio debug recording is enabled for users.
## Value Operation
## 0 Audio debug recording is disabled (default)

```

```

## 1 Audio debug recording is enabled
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R6.3 and later
## H1xx SIP R1.0 and later
## SET ENABLE_RECORDING 1
##
## WARNING_FILE specifies the file name or URL for a custom single-channel WAV file
## coded in ITU-T G.711 u-law or A-law PCM with 8-bit samples at 8kHz to be used
## as a call recording warning instead of the built-in English warning.
## The value can contain 0 to 255 characters; the default value is null ("").
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
## 96x1 SIP R6.3 and later
## SET WARNING_FILE "Warning.wav"
##
##### SECURE SHELL (SSH) SETTINGS #####
##
## Note: The SSH server on the endpoints is used by Avaya Services only for debugging purposes only.
## The SSH server supports only Avaya Services Logins ("craft" and "sroot").
## By enabling Avaya Services Logins you are granting Avaya access to your endpoints.
## This is necessary required to maximize the performance and value of your Avaya
## support entitlements, allowing Avaya to resolve product issues in a timely manner.
## In addition to enabling the Avaya Logins, the Avaya Product that the endpoints register with must be registered
## using the Avaya Global Registration Tool (GRT, see https://grt.avaya.com) to be eligible for Avaya remote connectivity.
## Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products
## and establishing remote access and alarming.
## By disabling Avaya Services Logins you are preventing Avaya access to
## your endpoints. 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. Endpoints that support EASG are no longer support ASG.
## EASG is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later ("craft" only)
## Avaya Vantage Devices SIP R1.0.0.0 and later ("craft" and "sroot").
## 96x1 SIP R7.1.0.0 and later ("craft" only)
##
## SSH_ALLOWED specifies whether SSH is supported.
## Value Operation
## 0 Disabled
## 1 Enabled
## 2 Configured using local craft procedure - the SSH server can be enabled or disabled from local craft procedure.
## When this mode is configured, then by default the SSH server is disabled.
## The default of 96x1 H.323 R6.2 up to 6.4 (not included) is 0 (disabled). The default value for 96x1 H.323 6.4 and later is 2.
## The default of 96x1 SIP R6.2 and later is 0 (disabled).
## The default of B189 is 0 (disabled).
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later (values 0-2), the default is 0.
## J169/J179 SIP R1.5.0 (values 0-2)
## Avaya Vantage Devices SIP R1.0.0.0 and later (values 0-1, default value is 0)
## 96x1 H.323 R6.2 and later (values 0-1), value 2 is added in R6.4 and later.
## 96x1 SIP R6.2 and later (values 0-1)
## B189 H.323 R1.0 and later (values 0-1)
## H1xx SIP R1.0 and later (values 0-1, default==0)
## SET SSH_ALLOWED 1
##
## SSH_BANNER_FILE specifies the file name or URL for a custom SSH banner file.
## If the value is null, a default English banner will be used for SSH.
## The value can contain 0 to 255 characters; the default value is null ("").
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later
## 96x1 H.323 R6.2 and later
## 96x1 SIP R6.2 and later
## B189 H.323 R1.0 and later

```

```

## H1xx SIP R1.0 and later
## SET SSH_BANNER_FILE http://security.myco.com/files/SSH-Banner.txt
##
## SSH_IDLE_TIMEOUT specifies the number of minutes of inactivity
## after which an SSH connection will be terminated
## Valid values are 0 through 32767; the default value is 10.
## A value of 0 means that the connection will not be terminated due to inactivity.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later
## 96x1 H.323 R6.2 and later
## 96x1 SIP R6.2 and later
## B189 H.323 R1.0 and later
## H1xx SIP R1.0 and later
## SET SSH_IDLE_TIMEOUT 30
##
## EASG_SITE_CERTS specifies list of EASG site certificates which are used by
## technicians when they don't have access to the Avaya network to generate
## EASG responses for SSH login.
## 0 to 255 ASCII characters: zero or more file names or URLs, separated by commas
## without any intervening spaces
## The default is "".
## This parameter is supported by:
## J129 SIP R1.1.0.0, J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 (build 2304) and later
## 96x1 SIP 7.1.0.0 and later
## SET EASG_SITE_CERTS "mySiteCert.p7b"
##
## EASG_SITE_AUTH_FACTOR specifies Site Authentication Factor code associated with
## the EASG site certificate being installed.
## Valid value: a 10 to 20 character alphanumeric string
## Default value: ""
## This parameter is supported by:
## J129 SIP R1.1.0.0, J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 (build 2304) and later
## 96x1 SIP 7.1.0.0 and later
## SET EASG_SITE_AUTH_FACTOR "avaya12345abcd"
##
## CERT_WARNING_DAYS_EASG specifies how many days before the expiration of
## EASG product certificate that a warning should first appear on the phone
## screen. Syslog message will be generated as well.
## Valid values are: 90-730, default is 365 days.
## This parameter is supported by:
## J129 SIP R1.1.0.0, J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP 7.1.0.0 and later
## SET CERT_WARNING_DAYS_EASG 100
##

##### Enhanced Debugging Capabilities Support #####
##
## AUTHCTRLSTAT controls whether enhanced debugging capabilities can be activated from the SSH server by
## Avaya technicians only. The parameter shall only be set to 1 for the debugging period by Avaya technicians and
## shall be configured back to 0 when the debugging period is end.
## Value Operation
## 0 Enhanced debugging capabilities are disabled (default).
## 1 Enhanced debugging capabilities are enabled.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.0.0.0 and later; While this parameter is supported, Avaya Technician is NOT expected
## to use it in the field and customers are encouraged to verify it is remain with its default value.
## 96x1 SIP R7.0.1.0 and later releases (hardware version 3 and up).
## 96x1 H.323 R6.2 and later releases (hardware version 3 and up).
## SET AUTHCTRLSTAT 1
##

##### SERVICE LEVEL AGREEMENT (SLA) MONITOR SETTINGS #####
##
## Please note that SLA Monitor agent requires specification of the root

```

```

## (and intermediate if applicable) trusted certificates using TRUSTCERTS for verifying
## the SLA Monitor server certificate.
##
## SLMSTAT specifies whether or not the SLA Monitor agent is enabled.
## Value Operation
## 0 Disabled (default)
## 1 Enabled
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later
## 96x1 H.323 R6.4 and later
## 96x1 SIP R6.2 and later
## 96x0 H.323 R3.1.4 and later
## SET SLMSTAT 1
##
## SLMCAP specifies whether the SLA Monitor agent is enabled for packet capture (sniffing).
## Value Operation
## 0 Disabled (default)
## 1 Enabled with payloads are removed from RTP packets
## 2 Enabled with payloads included in RTP packets
## 3 Controlled from craft menu - enable of RTP packets capture or disable packets capture
## using local CRAFT procedures.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later (values 0-3)
## 96x1 H.323 R6.4 and later (values 0-3)
## 96x1 SIP R6.2 to R6.5 (values 0-2)
## 96x1 SIP R7.0 and later (values 0-3)
## 96x0 H.323 R3.1.4 and later (values 0-2)
## SET SLMCAP 1
##
## SLMCTRL specifies whether the SLA Monitor agent is enabled for device control.
## Value Operation
## 0 Disabled (default)
## 1 Enabled
## 2 Controlled from craft menu
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later (values 0-2)
## 96x1 H.323 R6.4 and later (values 0-2)
## 96x1 SIP R6.2 to R6.5 (values 0-1)
## 96x1 SIP R7.0 and later (values 0-2)
## 96x0 H.323 R3.1.4 and later (values 0-1)
## SET SLMCTRL 1
##
## SLMPERF specifies whether the SLA Monitor agent is enabled for device performance monitoring.
## Value Operation
## 0 Disabled (default)
## 1 Enabled
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later
## 96x1 H.323 R6.4 and later
## 96x1 SIP R6.2 and later
## 96x0 H.323 R3.1.4 and later
## SET SLMPERF 1
##
## SLMPORT specifies the UDP port that will be opened by the SLA Monitor agent
## to receive discovery and test request messages.
## Valid values are 6000 through 65535; the default value is 50011.
## Important note: If default port is not used, both the SLA Mon agent and server must
## be configured with the SAME port. SLMPORT impacts the phone's SLA Mon agent configuration.
## A corresponding configuration must also be made on the SLA Mon server agentcom-slamon.conf file.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later
## 96x1 H.323 R6.4 and later
## 96x1 SIP R6.2 and later
## 96x0 H.323 R3.1.4 and later
## SET SLMPORT 43210
##
## SLMSEVR specifies the IP address and the port number of the SLA Mon server in the
## aaa.bbb.ccc.ddd:n format.

```

```

## Set the IP address of the SLA Mon server in the aaa.bbb.ccc.ddd format
## to restrict the registration of agents only to that server. Specifying a port
## number is optional. If you do not specify a port number, the system takes
## 50011 as the default port. If the value of the port number is 0, any port number is acceptable.
## The IP address must be in the dotted decimal format, optionally followed by a
## colon and an integer port number from 0 to 65535.
## To use a non-default port n, set the value of SLMSRVR in the
## aaa.bbb.ccc.ddd:n format, where aaa.bbb.ccc.ddd is the IP address
## of the SLA Mon server.
## Important note: If default port is not used, both the SLA Mon agent and server must
## be configured with the SAME port. SLMSRVR impacts the phone's SLA Mon agent configuration.
## A corresponding configuration must also be made on the SLA Mon server agentcom-slamon.conf file.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later
##   96x1 H.323 R6.4 and later
##   96x1 SIP R6.2 and later
##   96x0 H.323 R3.1.4 and later
## SET SLMSRVR 192.168.27.35:50011

##### ENHANCED LOCAL DIALING RULES #####
##
## These settings affect certain dialing behaviors, such as
## dialing numbers from the incoming Call Log or from web pages
## Please note that the enhanced local dialing rules are not applicable
## when using 96x0/96x1 H.323 phones in IP office environment.
##
##   Dialing Algorithm Status
##   Controls whether algorithm defined by parameters in
##   this section is used during certain dialing behaviors.
##   0 disables algorithm.
##   1 enables algorithm, but not for Contacts (default). For B189 H.323 only, value 1 has the same meaning as value 0
##   since B189 does not support call log application and WML browser.
##   2 enables algorithm, including Contacts (96xx SIP R2.0 and later, J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP
##   R2.0.0.0 and later,
##   96x1 SIP R6.0 and later, 96x1/B189 H.323 6.6 and later, H1xx SIP R1.0 and later)
##   Note: Avaya Vantage Basic Application SIP R1.0.0.1 and later and Avaya Equinox 3.1.2 and later support values 0 (disabled) and 1
##   where value means that enhanced local dialing rules are applied on
##   all outgoing calls (whether originated from contacts, history or dialer). All Enhanced local dialing rules parameters mentioned in
##   this section which are marked as supported
##   by Avaya Vantage Basic application SIP R1.0.0.1 and later and Avaya Equinox 3.1.2 and later can be supported by any Avaya
##   Breeze Client SDK based application.
## SET ENHDIALSTAT 1
##
##   Country Code
##   For United States the value is '1'
##   Valid values 1 to 999. The default value is 1.
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   Avaya Equinox 3.1.2 and later; default is "".
##   Avaya Vantage Basic Application SIP R1.0.0.1 and later; default is "".
##   H1xx SIP R1.0 and later
##   96x1 H.323 R6.0 and later
##   96x1 SIP R6.0 and later
##   96x0 H.323 R1.0 and later
##   96x0 SIP R2.5 and later
## SET PHNCC 1
##
##   Internal extension number length
##   If your extension is 12345, your dial plan length is 5.
##   On 96xx phones, the maximum extension length is 13.
##   This value must match the extension length set on your
##   call server.
##   Valid values are 3-13. The default value is 5.
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   Avaya Equinox 3.1.2 and later; default is "".
##   Avaya Vantage Basic Application SIP R1.0.0.1 and later; default is "".
##   H1xx SIP R1.0 and later
##   96x1 H.323 R6.0 and later
##   96x1 SIP R6.0 and later

```



```

## 96x0 H.323 R1.0 and later
## 96x0 SIP R2.5 and later
## SET PHNDPLENGTH 5
##
## International access code
## For the United States, the value is 011.
## Valid values are 0 to 4 dialable characters (0-9,*,#). The default value is "011".
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Equinox 3.1.2 and later; default is "".
## Avaya Vantage Basic Application SIP R1.0.0.1 and later; default is "".
## H1xx SIP R1.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R2.5 and later
## SET PHNIC 011
##
## Long distance access code
## Valid values are 0 through 9 and empty string. The default value is 1.
## if no long distance access code is needed then SET PHNLD "".
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Equinox 3.1.2 and later; default is "".
## Avaya Vantage Basic Application SIP R1.0.0.1 and later; default is "".
## H1xx SIP R1.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R2.5 and later
## SET PHNLD 1
##
## National telephone number Length
## For example, 800-555-1111 has a length of 10.
## Valid values are 5-15. The default value is 10.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Equinox 3.1.2 and later; default is "".
## Avaya Vantage Basic Application SIP R1.0.0.1 and later; default is "".
## H1xx SIP R1.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R2.5 and later
## SET PHNLDLENGTH 10
##
## Outside line access code
## The number you press to make an outside call.
## Valid values are 0 to 2 dialable characters (0-9, *, #). The default value is 9.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Equinox 3.1.2 and later; default is "".
## Avaya Vantage Basic Application SIP R1.0.0.1 and later; default is "".
## H1xx SIP R1.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R2.5 and later
## SET PHNOL 9
##
## ELD_SYSNUM
## Controls whether Enhanced Local Dialing algorithm will be
## applied for System Numbers - Busy Indicators and Auto Dials.
## Value Operation
## 0 Disable ELD for System Numbers
## 1 Enable ELD for System Numbers (Default)
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)

```



```

## 96x1 SIP R7.0.1.2 and later.
##
## SET ELD_SYSNUM 1

##### AUDIO SETTINGS #####
##
## Automatic Gain Control (AGC).
## These settings enable or disable AGC.
##
## A value of 1 (default) enables AGC. A value of 0 disables AGC.
## AGCHAND controls handset AGC.
## AGCHEAD controls headset AGC
## AGCSPKR controls speaker AGC.
## Note: AGCHAND, AGCHEAD and AGCSPKR are supported by H1xx SIP R1.0 and later and Avaya Vantage Devices SIP R1.0.0.0 and later.
## Note: AGCHAND and AGCSPKR are supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later. AGCHEAD is supported by J100 SIP R2.0.0.0 and later (J169/J179 only).
## Note: For 96x1 H.323 - User can also change the "Handset/Headset/Speaker Auto Gain Control" fields
## in HOME-> Options & Settings-> Advanced Options -> Automatic Gain Control... menu.
## AGCHAND/AGCHEAD/AGCSPKR will be enforced only in case user did not change at all the relevant "Handset/Headset/Speaker Auto Gain Control" field value.
## Please note that user changes are stored in backup/restore file as "Handset AGC", "Headset AGC" and "Speaker AGC" (if BRURI has a valid value) which means that if the
## restored file include "Handset AGC", "Headset AGC" and/or "Speaker AGC" parameters then they will take precedence over AGCHAND, AGCHEAD and AGCSPKR respectively.
## If BRURI is not valid, but user still change the content of "Handset/Headset/Speaker Auto Gain Control" fields, then user value will take precedence over
## AGCHAND, AGCHEAD and AGCSPKR respectively. The only way to clear user configuration in this case is by doing:
## a. "CLEAR" operation in CRAFT menu,
## b. New user login.
## SET AGCHAND 0
## SET AGCHEAD 0
## SET AGCSPKR 0
##
## Audio Environment Index
## Enables you to customize the telephone's audio
## performance. (0-299) This parameter affects settings
## for AGC dynamic range, handset and headset noise
## reduction thresholds, and headset transmit gain. It is
## highly recommended you consult Avaya before changing
## this parameter.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0 and J100 SIP R2.0.0.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## 96x0 H.323 "0" through "80" (R1.0, R1.1), "0" through "191" (R1.2 - R1.5), "0" through "299" (R2.0+)
## 96x0 SIP R2.6 and later
## SET AUDIOENV 0
##
##### CUSTOM RING TONES #####
##
## RINGTONESTYLE specifies the style of ring tones that are offered to the user
## for Personalized Ringing when "Classic" (as opposed to "Rich") is selected.
## Value Operation
## 0 North American ring tones are offered (default)
## 1 European ring tones are offered
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.1.0.0 and later
## 9670 H.323 R2.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.3 and later
## H1xx SIP R1.0 and later
## H1xx SIP R1.0 and later
## SET RINGTONESTYLE 1
##
## RINGTONES specifies a list of display names and file names or URLs
## for a custom ring tone files to be downloaded and offered to users.

```

```

## The list can contain 0 to 1023 UTF-8 characters; the default value is null ("").
## Values are separated by commas without any intervening spaces.
## Each value consists of a display name followed by an equals sign followed by a file name or URL.
## Display names may contain spaces, but if any do, the entire list must be quoted.
## Ring tone files must be single-channel WAV files
## coded in ITU-T G.711 u-law or A-law PCM with 8-bit samples at 8kHz.
## This parameter is supported by:
##   Avaya Vantage Devices SIP R1.1.0.0 and later; please note that the format is list of file names or URLs (without display name).
##   J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
##   96x1 SIP R6.3 and later
##   H1xx SIP R1.0 and later
## SET RINGTONES "Steam Whistle=tones/swhistle.wav,Car Horn=tones/chorn.wav,Siren=tones/siren.wav"
## Example for Avaya Vantage:
## SET RINGTONES "tones/swhistle.wav,tones/chorn.wav,tones/siren.wav"
## Note: In order to set RINGTONES for Avaya Vantage and other phones then shall be use of the IF conditional statement (e.g. IF
$MODEL4 SEQ K175 GOTO SETTINGSK1XX)
## with $MODEL4 to separate between K175/K165 to other phones.
##
## RINGTONES_UPDATE specifies whether the phone will query the file server to determine whether
## there is an updated version of each custom ring tone file each time the phone starts up or resets.
## Value Operation
## 0 Phone will only try to download ring tones with new display names (default)
## 1 Phone will check for updated version of each ring tone file at startup
## This parameter is supported by:
##   J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (J169/J179 only)
##   96x1 SIP R6.3 and later.
## SET RINGTONES_UPDATE 1
##

##### FILE SERVER SETTINGS #####
##
## HTTP Server Addresses
## [If you set your HTTP Server Addresses via DHCP, do not
## set them here as they will override your DHCP settings.
## Server used to download configuration script files.
## Zero or more HTTP server IP addresses in dotted-decimal,
## colon-hex (96x1 H.323 R6.0 onwards), or DNS name format,
## separated by commas without any intervening spaces.
## (0 to 255 ASCII characters, including commas).
## This parameter may also be changed via LLDP.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   Avaya Vantage Devices SIP R1.0.0.0 and later
##   H1xx SIP R1.0 and later
##   96x1 H.323 R6.0 and later
##   96x1 SIP R6.0 and later
##   B189 H.323 R1.0 and later
##   96x0 H.323 R1.0 and later
##   96x0 SIP R1.0 and later
## SET HTTPSRVR 192.168.0.5
##
## HTTP Server Directory Path
## Specifies the path name to prepend to all file names
## used in HTTP and HTTPS GET operations during startup.
## (0 to 127 ASCII characters, no spaces.)
## Note: This parameter is also supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later.
## SET HTTPDIR myhttpdir
##
## HTTP port
## Sets the TCP port used for HTTP file downloads from
## non-Avaya servers. (0-65535) The default value is 80.
## Applies only to 96xx phones, 96x1 phones, J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later.
## SET HTTPPORT 80
##

## Server Authentication
## Sets whether script files are downloaded from an
## authenticated server over an HTTPS link.

```

```

## 0 for optional, 1 for mandatory
## Note: This parameter is also supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later,
## H1xx SIP R1.0 and later and Avaya Vantage Devices SIP R1.0.0.0 and later.
## SET AUTH 0
##
## HTTPS Server Addresses
## [If you set your HTTP/S Server Addresses via DHCP, do not
## set them here as they will override your DHCP settings.
## Server used to download configuration script files.
## Zero or more HTTPS server IP addresses in dotted-decimal,
## colon-hex (96x1 H.323 R6.0 onwards), or DNS name format,
## separated by commas without any intervening spaces.
## (0 to 255 ASCII characters, including commas).
## This parameter may also be changed via LLDP.
## J129 SIP R1.1.0.0, J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.1.0.0 and later
## H1xx SIP R1.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R7.1.0.0 and later
## B189 H.323 R1.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## SET TLSSRV 192.168.0.5
##
## HTTPS Server Directory Path
## Specifies the path name to prepend to all file names
## used in HTTPS GET operations during startup.
## (0 to 127 ASCII characters, no spaces.)
## Note: This parameter is also supported by J129 SIP R1.1.0.0, J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later.
## SET TLSDIR myhttpdir
##
## HTTPS port
## Sets the port used for HTTPS file downloads from
## non-Avaya servers. (0-65535) The default value is 443.
## Note: This parameter is also supported by J129 SIP R1.1.0.0, J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later.
## SET TLSPT 443
##
##### DEVICE ENROLLMENT SERVICE (DES) #####
##
## DES_STAT Specifies if DES discovery is to be attempted during the boot process if there is no configuration file server provisioned on
the phone.
## Value Operation
## 0 DES discovery is disabled and can only be restored with Reset to Defaults
## 1 DES discovery is disabled
## 2 DES discovery is enabled (default)
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later
## Avaya Vantage Devices SIP R1.1.0.0 and later; if FILE_SERVER_URL/HTTPSRVR/TLSSRV are received from
DHCP/LLDP/UI/configuration file/AADS then DES will not be activated.
## SET DES_STAT 1
##

##### RTCP MONITORING #####
##
## The RTCP monitor
## One RTCP monitor (VMM server) IP address in
## dotted-decimal format or DNS name format (0 to 15
## characters). Note that for H.323 telephones only this
## parameter may be changed via signaling from Avaya
## Communication Manager. For 96xx/J100 SIP models in Avaya Aura
## environments, this parameter is set via the PPM server.
## Note : This setting is supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later, H1xx SIP R1.0
and later
## for non-Aura environment (For example: IP Office, etc).
## SET RTCPMON 192.168.0.10
##
## RTCPMONPORT sets the port used to send RTCP information
## to the IP address specified in the RTCPMON parameter.

```

```

## RTCPMONPORT is only supported on 96xx/J100 in non-Avaya environments. For 96xx/J100 SIP
## models in Avaya environments, this parameter is set via the PPM server. The default value is 5005.
## Note : This setting is supported by H1xx SIP R1.0 and later and J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## for non-Aura environment (For example: IP Office, etc).
## SET RTCPMONPORT 5005
##
## RTCP Monitor Report Period
## Specifies the interval for sending out RTCP monitoring
## reports (5-30 seconds). Default is 5 seconds. This
## parameter applies only to 96xx/J100 SIP telephones.
## Note : This setting is supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## for non-Aura environment (For example: IP Office, etc).
## SET RTCPMONPERIOD 5
##
##### ICMP SETTINGS #####
##
## Destination Unreachable Message Control
## Controls whether ICMP Destination Unreachable messages
## are generated.
## 0 for No
## 1 for limited Port Unreachable messages
## 2 for Protocol and Port Unreachable messages
## Note 1: This settings is also applicable for J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later, H1xx SIP
## R1.0 and later and
## Avaya Vantage Devices SIP R1.0.0.0 and later.
## SET ICMPDU 1
##
## Redirect Message control
## Controls whether received ICMP Redirect messages will
## be processed
## 0 for No
## 1 for Yes
## Note 1: This settings is also applicable for J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later, H1xx SIP
## R1.0 and later and
## Avaya Vantage Devices SIP R1.0.0.0 and later.
## SET ICMPRED 0
##
##### BACKUP/RESTORE SETTINGS (H.323 and SIP) #####
##
## Backup and Restore URI
## URI used for HTTP backup and retrieval of user data.
## Specify HTTP server and directory path to backup file.
## Do not specify backup file name.
## Note: This parameter is supported by 96x1 H323 R6.2.3 and later, J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later, H1xx
## SIP R1.0 and later and 96x1 SIP R7.1.0.0 and later releases
## for sending a phone report to a HTTP/S file server (with the URI of the server defined by the BRURI parameter).
## In order to send the report the phone must be registered and the administrator must access the
## phone's Admin menu and select the Send Report feature. This parameter is supported in both IPO and Aura environment with file
## server that support HTTP PUT messages.
## SET BRURI http://192.168.0.28
## Note: 96x0 H.323 R3.2/96x1 H.323 R6.0 phones support in addition a format of "http://username:password@..." or
## "https://username:password@..." for HTTP Basic authentication.
## The username and password are removed from the configured URI and used in the Authorization Header. The HTTP request will be
## sent to the URI without the username and password fields.
## For example:
## SET BRURI http://Administrator:Catt*123@10.10.10.6/Backup/
## SET BRURI http://iphone:Avaya1234@10.10.10.1
##
## Backup/Restore Authentication
## Specifies whether authentication is used for backup/restore file download.
## Call server IP address and telephone's registration can be used as credentials.
## 0: Call server IP address and telephone's registration password
## are not included as credentials (Default).
## 1: The call server IP address and the telephone's registration
## password are included as the credentials in an Authorization request-header
## SET BRAUTH 0
##

```

```
##### AUDIBLE ALERTING #####
##
## Specifies the audible alerting setting for the telephone
## and whether users may change this setting.
##
## A value of 0 turns off audible alerting; user cannot
## adjust ringer volume at all.
## A value of 1 turns on audible alerting; user can adjust
## ringer volume but cannot turn off audible alerting.
## A value of 2 turns off audible alerting; user can adjust
## ringer volume and can turn off audible alerting.
## A value of 3 turns on audible alerting; user can adjust
## ringer volume and can turn off audible alerting.
##
## The default value is 3.
## SET AUDASYS 3
##
## Note: AUDASYS is not supported by J129 SIP R1.0.0.0/R1.1.0.0. Supported by J100 SIP R2.0.0.0 and later.

#####
##
## VOICE MAIL SETTINGS
##
#####
##
## Voice Mail Telephone Number
## Specifies the telephone number to be dialed
## automatically when the telephone user presses the
## Messaging button. The specified number is used to
## connect to the user's Voice Mail system.
## Note: PSTN_VM_NUM shall be used instead of MSGNUM in cases of IP Office environment, 3PCC SIP environment or when there is
## failover from Aura environment to a non-Aura server.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later
## H1xx SIP R1.0 and later
## 96x1 H.323 R6.0 and later
## 96x1 SIP R6.0 and later
## 96x0 H.323 R1.0 and later
## 96x0 SIP R1.0 and later
## Example:
## SET MSGNUM 1234

#####
## IPv6 related settings are applicable for 96x1 H.323 R6.0 and later, 96x1 SIP R7.1.0.0 and later and J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later support only IPV6STAT.
##

##
## DHCPSTAT
## Valid Values
## 1 run DHCPv4 only (IPv4only-mode, if no own IPv6 address is programmed statically), Default.
## 2 run DHCPv6 only (IPv6only-mode, if no own IPv4 address is programmed statically)
## 3 run both DHCPv4 & DHCPv6 (dual-stack mode)
## Description
## Specifies whether DHCPv4, DHCPv6, or both will be used in case IPV6STAT has enabled IPv6 support generally
## Example : Setting dual stack mode
## SET DHCPSTAT 3
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later; Value 1 as described above, Value 2/3 - run both DHCPv4 & DHCPv6
## 96x1 H.323 R6.0 and R6.0
## SET DHCPSTAT 1
##

## IPV6STAT
## Valid Values
```

```
## 0 IPv6 will not be supported.
## 1 IPv6 will be supported.
## Description
## Specifies whether IPv6 will be supported
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later (Default is 0).
## Avaya Vantage Devices SIP R1.0.0.0 and later; (Default is 1); IPV6STAT shall be set to 0 as IPv6 is not supported by Avaya
Vantage Device.
## 96x1 H.323 R6.0 and R6.0 (Default is 0).
## 96x1 SIP R7.1.0.0 and later (Default is 0).
## SET IPV6STAT 1
##
## SIGNALING_ADDR_MODE
## Valid Values
## 4 IPv4 (default)
## 6 IPv6
## Description
## This parameter is used by SIP signaling on a dual mode phone (phone with both IPv4 and IPv6 addresses configured) to select the
preferred SIP controller IP addresses
## from SIP_CONTROLLER_LIST_2. The phone registers to SIP controllers using IPv4 address if SIGNALING_ADDR_MODE=4,
## otherwise registration is over IPv6.
## The single IPv4 mode phone ignores SIGNALING_ADDR_MODE and SIP_CONTROLLER_LIST_2 and selects the SIP controller's IP
addresses from SIP_CONTROLLER_LIST.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## Example:
## SET SIGNALING_ADDR_MODE 4
##
## MEDIA_NEG_PREFERENCE
## Valid Values
## 0 Remote or offerer's precedence (default)
## 1 Local
## NOTE: MEDIA_NEG_PREFERENCE is NOT used in Avaya environment. Default is remote preference.
## It is used by a dual mode answerer in non-Avaya environment to allow a local preference
## It is used in non-Avaya environment to allow a local preference.
## NOTE: Not applicable on single mode phones.
## Description
## MEDIA_NEG_PREFERENCE option is used by the answerer only to change the default address
family preference.
## In dual IPv4/IPv6 mode, during SIP ANAT negotiation,
## MEDIA_NEG_PREFERENCE is used to prioritize media lines in SDP.
## By default offerer's preference is used.
##
## MEDIA_NEG_PREFERENCE of zero means when there is a choice between IPv4 and IPv6 address,
## the answerer honors the offerer's preference.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## Example
## SET MEDIA_NEG_PREFERENCE 0
##
## MEDIA_ADDR_MODE
## Valid Values
## 4 IPv4 (default)
## 6 IPv6
## 46 Prefer IPv4 over IPv6
## 64 Prefer IPv6 over IPv4
## Description
## MEDIA_ADDR_MODE specifies the preference of SDP media group lines [per RFC 4091, 4092 and 5888] and the SDP answer / offer
format.
## By default v4 media line is preferred.
## MEDIA_ADDR_MODE is only used by dual stack phones which are configured with both IPv4 and IPv6 addresses.
## IPv4 only or IPv6 only phones ignores MEDIA_ADDR_MODE.
## Environment SDP Offer SDP Answer (Note2)
## Avaya 4 - Non ANAT IPv4 only is advertised (Note 3) 4 - IPv4 is chosen (see Note1,3)
## 6 - Non ANAT IPv6 only is advertised (Note 3) 6 - IPv6 is chosen (see Note1,3)
## 46 - ANAT offer where IPv4 is preferred over IPv6 46 - Follow the remote preference.
```

```

##          64- ANAT offer where IPv6 is preferred over IPv4      64 – Follow the remote preference.
## Non-Avaya          Same as for Avaya environment          4 – IPv4 is chosen (see Note1,3)
##          6 – IPv6 is chosen (see Note1,3)
##          46 – Prefer IPv4 (if available in SDP offer) only if MEDIA_NEG_PREFERENCE
##                                     is set to local,
otherwise grants the remote preference.
##          64 – Prefer IPv6 (if available in SDP offer) only if MEDIA_NEG_PREFERENCE
##                                     is set to local, otherwise grants the
remote preference.
## Note1: MEDIA_ADDR_MODE=4 and 6 answerers select the MEDIA_ADDR_MODE address family in ANAT offer.
## For non-ANAT offers or ANAT offers with selected "m" line (e.g. re-INVITE), answerers reject the call
## with 488, if MEDIA_ADDR_MODE does not match any of offered audio lines (with non-zero port).
## NOTE2: Answerers are always ANAT capable.
## NOTE3: MEDIA_ADDR_MODE 4 or 6 enforces a dual stack phones which are configured with both IPv4 and IPv6 address to behave
as IPv4 only or IPv6 only phone.
## MEDIA_NEG_PREFERENCE is ignored when MEDIA_ADDR_MODE is 4 or 6.
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## Example : Setting to use IPv6 only
## SET MEDIA_ADDR_MODE 6
## Example : Setting to preference of IPv6 over IPv4
## SET MEDIA_ADDR_MODE
##
## IPV6DADXMITS specifies whether Duplicate Address Detection is performed
## on tentative addresses, as specified in RFC 4862.
## Non zero value specifies the maximum number of transmitted Neighbor Solicitation messages
## to determine whether an IPv6 address is already in use.
## Value Operation
## 0 DAD is disabled
## 1-5 maximum number of transmitted NS messages
## Default value is 1
## This parameter is supported by:
## This parameter is supported by:
## J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## Example:
## SET IPV6DADXMITS 1
##

#####
##
## SIP SETTINGS
## Settings applicable only to 96xx/J100 telephone models
## in non-Avaya environments
##
#####
## CALLFWDSTAT sets the call forwarding mode of the set by summing the values below:
## 1 Permits unconditional call forwarding
## 2 Permits call forward on busy
## 4 Permits call forward/no answer
## A value of 0 disables call forwarding.
## The default is 0.
## Example: a value of 6 allows Call Forwarding on busy and on no answer.
## Note: This parameter is supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later for IP Office Environment.
## SET CALLFWDSTAT 3
##
## CALLFWDDELAY sets the number of ring cycles before the
## call is forwarded to the forward or coverage address.
## The default delay is one ring cycle.
## Note: This parameter is supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later for IP Office Environment. The
range is 0 to 20 with Default is 1.
## SET CALLFWDDELAY 5
##
## CALLFWDADDR sets the address to which calls are forwarded for the call forwarding feature.
## The default is null ("").
## Note the user can change or replace this administered value if CALLFWDSTAT is not 0.

```



```

## Note: This parameter is supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later for IP Office Environment.
## SET CALLFWDADDR cover@avaya.com
##
## COVERAGEADDR sets the address to which calls will be forwarded for the call coverage feature.
## The default is null ("").
## Note the user can change or replace this administered value if CALLFWDSTAT is not 0.
## This parameter is not supported for 3PCC environment.
## SET COVERAGEADDR cover@avaya.com
##
## SIPCONFERENCECONTINUE specifies whether a conference call continues after the host hangs up.
## 0 for drop all parties (default)
## 1 for continue conference
## SET SIPCONFERENCECONTINUE 0
##
## ENABLE_AUTO_ANSWER_SUPPORT specifies whether the Auto Answer feature is available to users.
## Value Operation
## 0 Auto Answer feature is not available to users (default)
## 1 Auto Answer feature is available to users
## Note: This parameter is supported by J129 SIP R1.1.0.0, J100 SIP R2.0.0.0 and later only for 3PCC environment.
## SET ENABLE_AUTO_ANSWER_SUPPORT 1
##
## Auto Answer Mute controls the speakerphone muting when call is auto answered by phone.
## Value Operation
## 0 Speakerphone is Unmuted when Auto Answered
## 1 Speakerphone is Muted when Auto Answered (default)
## Note: This parameter is supported by J129 SIP R1.1.0.0, J100 SIP R2.0.0.0 and later only for 3PCC environment.
## SET AUTO_ANSWER_MUTE_ENABLE 0
##
## ENABLE_DND specifies whether the Do Not Disturb feature is available to users.
## Value Operation
## 0 Do Not Disturb feature is not available to users
## 1 Do Not Disturb feature is available to users (default)
## Note: This parameter is supported by J129 SIP R1.1.0.0, J100 SIP R2.0.0.0 and later only for 3PCC environment.
## SET ENABLE_DND 0
##
## DND_PRIORITY_OVER_CFU_CFB defines the priority between features Do Not Disturb and Call Forward Unconditional/Busy when
both are activated by user.
## Value Operation
## 0 Call Forward Unconditional/Busy feature has priority over Do Not Disturb feature (default)
## 1 Do Not Disturb feature has priority over Call Forward Unconditional/Busy feature
## Note: This parameter is supported by J129 SIP R1.1.0.0, J100 SIP R2.0.0.0 and later only for 3PCC environment.
## SET ENABLE_DND_PRIORITY_OVER_CFU_CFB 1
##
## HOLD_REMINDER_TIMER specifies the number of seconds after which the phone will alert (visual and audible) user when any call is
kept on hold.
## Valid values are 0 through 999 seconds; the default value is 0.
## Value 0 means phone will not alert user when any call is kept on hold.
## Note: This parameter is supported by J129 SIP R1.1.0.0, J100 SIP R2.0.0.0 and later only for 3PCC environment.
## SET HOLD_REMINDER_TIMER 60
##
## PROVIDE_TRANSFER_TYPE provides the call transfer type in 3rd party environments.
## No meaning for Avaya environment
## Value 0 or 1 (default 0)
## SET PROVIDE_TRANSFER_TYPE 0
##
## CALL_TRANSFER_MODE determines the call transfer mode in 3rd party environments.
## Value 0 or 1 (default is 0)
## SET CALL_TRANSFER_MODE 0
##
#####
## 96xx, J129, H1xx SIP SETTINGS
## Settings applicable only to 96xx, J100, and H1xx Video collaboration Station
## running the SIP protocol
##
#####
## Power over Ethernet conservation mode

```



```

## If POE_CONS_SUPPORT is set to 1 then Power conservation mode is supported.
## If this parameter is set to 0 then Power conservation mode is not supported.
## Note: Not supported by H1xx SIP and J129 SIP.
## SET POE_CONS_SUPPORT 1
##
## Personalize button labels ability
## CNGLABEL determines ability to personalize button labels to be displayed to
## the user. If it is set to 0 then ability will not be displayed to user.
## If it is set to 1 then personalize button labels ability will be exposed to user.
## Default value is 1.
## Note: Not supported by H1xx SIP and J129 SIP.
## SET CNGLABEL 1.
##
## Selection of Conference Method
## If CONFERENCE_TYPE is set to 0 then local conferencing is supported based on
## sipping services. If set to 1 then server based conferencing is supported.
## If it is set to 2 then click-to conference server based conferencing is supported.
## If it is set to outside range then default value is selected.
## Default value is 1.
## Note: Not supported by H1xx SIP. Supported by J100 SIP R2.0.0.0 and later.
## SET CONFERENCE_TYPE 1
##
## Call Coverage Tone
## Specifies the tone to play when a call goes to
## coverage. The default is 1 and valid values are 1-4.
## SET REDIRECT_TONE 1
##
## ENABLE_EARLY_MEDIA specifies whether the phone sets up a voice channel
## to the called party before the call is answered.
## Setting this parameter to 1 can speed up call setup.
## 0 for No
## 1 for Yes
## SET ENABLE_EARLY_MEDIA 1
##
## USE_QUAD_ZEROES_FOR_HOLD specifies the method to use to indicate that a call is on hold.
## A setting of 1 is useful for compatibility with 3rd party SIP endpoints.
## 0 for "a= directional attributes"
## 1 for 0.0.0.0 IP address
## SET USE_QUAD_ZEROES_FOR_HOLD 0
##
## RTCPCONT specifies whether the sending of RTCP is enabled.
## 0 for No
## 1 for Yes
## SET RTCPCONT 1
##
## RTCP_XR specifies whether VoIP Metrics Report Block as defined in RTP Control Protocol Extended Reports (RTCP XR)
## (RFC 3611) is sent as part of RTCP packets to remote peer or to RTCP monitoring server.
## 0 for No (Default)
## 1 for Yes
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.0.0 and later
## SET RTCP_XR 1
##
## MTU_SIZE specifies the maximum transmission unit (MTU) size transmitted by the phone.
## Valid values are 1496 or 1500.
## Use 1496 for older Ethernet switches.
## Note: This parameter is also applicable for H1xx SIP R1.0 and later and for Avaya Vantage Devices SIP R1.0.0.0 and later
## for Ethernet interface only (not Wi-Fi interface where the MTU is fixed 1500 bytes).
## SET MTU_SIZE 1500
##
## MEDIAENCRYPTION specifies which media encryption (SRTP) options will be supported.
## Up to 2 or 3 options may be specified in a comma-separated list.
## 2 options are supported by:
## 1. Prior releases to 96x1 SIP 7.0.0
## 2. H1xx SIP R1.0 and later
## 3. 96x0 SIP R1.0 to R2.6.14.1

```

```

## 3 options are supported by 96x1 SIP R7.0.0 and later, J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later and H1xx SIP R1.0.1 and later.
## For 96x0 SIP R2.6.14.5 and later, up to 3 options may be specified, but only the first two supported options are used.
## Options should match those specified in CM IP-codec-set form.
## 1 = aescm128-hmac80
## 2 = aescm128-hmac32
## 3 = aescm128-hmac80-unauth
## 4 = aescm128-hmac32-unauth
## 5 = aescm128-hmac80-unenc
## 6 = aescm128-hmac32-unenc
## 7 = aescm128-hmac80-unenc-unauth
## 8 = aescm128-hmac32-unenc-unauth
## 9 = none (default)
## 10 = aescm256-hmac80
## 11 = aescm256-hmac32
## Options 10 and 11 are supported by 96x1 SIP R7.0.0 and later, H1xx SIP R1.0.1 and later and J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later.
## Note: The list of media encryption (SRTP) options is ordered from high (left) to the low (right) options. The phone will publish this list in the SDP-OFFER
## or choose from SDP-OFFER list according to the list order defined in MEDIAENCRYPTION. Please note that Avaya Communication Manager has the capability
## to change the list order in the SDP-OFFER (for audio only) when the SDP-OFFER pass through CM.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Equinox 3.1.2 and later; supported values: 1,2,9,10 and 11. The default value is 1,2,9.
## Avaya Vantage Basic Application SIP R1.0.0.0 and later; supported values: 1,2,9,10 and 11. The default value is 1,2,9.
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R1.0 and later
## SET MEDIAENCRYPTION 1,9
## SET MEDIAENCRYPTION 10,1,9
##
## ENCRYPT_SRTCP specifies whether RTCP packets are encrypted or not. SRTCP is only used if SRTP is enabled using
## MEDIAENCRYPTION (values other than 9 (none) are configured).
## This parameter controls RTCP encryption for RTCP packets exchanged between peers.
## RTCP packets sent to Voice Monitoring Tools are always sent unencrypted.
## Value Operation
## 0 SRTCP is disabled (default).
## 1 SRTCP is enabled.
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Equinox 3.1.2 and later
## 96x1 SIP R7.1.0.0 and later
## Avaya Vantage Basic Application SIP R1.0.0.0 and later
## SET ENCRYPT_SRTCP 1
##
## SUBSCRIBE_SECURITY specifies the use of SIP or SIPS for subscriptions.
## If SUBSCRIBE_SECURITY is 0, the phone uses SIP for both the Request URI and the
## Contact Header regardless of whether SRTP is enabled. If SUBSCRIBE_SECURITY is 1,
## the phone uses SIPS for both the Request URI and the Contact Header if SRTP is enabled
## (TLS is on and MEDIAENCRYPTION has at least one valid crypto suite).
## If SUBSCRIBE_SECURITY is 2, and the SES/PPM does not show a FS-DeviceData FeatureName
## with a FeatureVersion of 2 in the response to the getHomeCapabilities request
## For IP office environment, the applicable values are 0 and 1.
## SET SUBSCRIBE_SECURITY 2
##
##### IP OFFICE SETTINGS #####
##
## ENABLE_IPOFFICE specifies whether the deployment environment is IP Office
## Value Operation
## 0 Not IP Office environment (except failover mode to IP Office in Avaya Aura environment) (Default)
## 1 IP Office environment; Native support of IP Office with a limited feature set.
## 2 IP Office environment; Additional features driven by the IP Office SIP proxy.
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later (J129 supports values 0-1 and J169/J179 support values 0 and 2). When ENABLE_IPOFFICE is set to 2,
## some of the 46xxsettings.txt file parameters have no effect.
## Avaya Vantage Basic Application SIP R1.1.0.1 and later (values 0-1)
## Avaya Vantage Devices SIP R1.1.0.1 and later (values 0-1)
## J169/J179 SIP R1.5.0 (values 0-1)

```

```

## J129 SIP R1.0.0.0 (or R1.1.0.0) (values 0-1)
## H1xx SIP R1.0.2 and later (values 0-1)
## SET ENABLE_IPOFFICE 1
##
## MEDIA_PRESERVATION specifies whether a call will be preserved when there is no SIP connectivity to IP Office.
## This parameter is only applicable when ENABLE_IPOFFICE is set to 2.
## Value Operation
## 0 Phone will not preserve a call. As soon as the phone detects SIP connectivity failure to IP Office, phone will drop a call and make
re-registration attempt.
## 1 Phone will try to preserve a call for a duration specified by PRESERVED_CALL_DURATION settings parameter (Default).
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later
## SET MEDIA_PRESERVATION 0
##
## PRESERVED_CALL_DURATION specifies how long the call will be preserved if ENABLE_IPOFFICE is set to 2 and if
MEDIA_PRESERVATION is set to 1.
## In such case, the call will be preserved for a duration of PRESERVED_CALL_DURATION minutes. Valid values are 10-120. Default
value is 120 minutes.
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later
## SET PRESERVED_CALL_DURATION 10
##
## SUBSCRIBE_LIST_NON_AVAYA specifies comma separated list of event packages to subscribe to after registration.
## Possible values are: "reg", "dialog", "mwi", "ccs", "message-summary" which is identical to "mwi", "avaya-ccs-profile" which is
identical to "ccs"
## The values are case insensitive.
## For IPO the recommended value shall be "reg, message-summary, avaya-ccs-profile".
## For 3PCC environment the value "message-summary" may be required.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## Avaya Vantage Basic Application SIP R1.1.0.1 and later
## H1xx SIP R1.0.2 and later
## SET SUBSCRIBE_LIST_NON_AVAYA "reg, message-summary, avaya-ccs-profile"
##
## ENABLE_3PCC_ENVIRONMENT specifies whether the deployment environment is third party SIP Server
## Value Operation
## 0 Not 3PCC environment
## 1 3PCC environment (Default)
## Note: This parameter should be set to '0' for Aura environment and IP Office
## Note: This parameter is supported by J129 SIP R1.1.0.0 and J100 SIP R2.0.0.0 and later
## SET ENABLE_3PCC_ENVIRONMENT 0
##
## USER_STORE_URI for User Data
## URI used for HTTP/S backup and retrieval of user data.
## Specify HTTP/S server and directory path to backup file.
## Do not specify backup file name.
## This parameter is supported by:
## Avaya Vantage Devices SIP R1.1.0.1 and later
## J129 SIP R1.1.0.0, J100 SIP R2.0.0.0 and later
## SET USER_STORE_URI https://192.168.0.28
## Note: This parameter is supported by Avaya Vantage Devices SIP R1.1.0.1 and later to define user store URI for personal/enterprise
contacts. Used in IP Office environment only.
## The default ports are 80 for HTTP and 443 for HTTPS. When "Use Preferred Port" is enabled in IP Office 11.0 and later then the
ports are changed to 8411 for HTTP and 411 for HTTPS.
## SET USER_STORE_URI https://192.168.0.28:411
## SET USER_STORE_URI http://192.168.0.28:8411
## Note: This parameter is supported by J129 SIP R1.1.0.0, J100 SIP R2.0.0.0 and later for 3PCC Environment and IP Office R10.1 and
later.

##### DISPLAY SETTINGS #####
##

##
## Display Logo (96x1) / Wallpaper (H1xx/Avaya Vantage)
## Specifies a list of tuples describing logo/wallpaper used as phone
## display background. See Administrator's guide for
## additional detail.
## This parameter is supported by:

```

```
## J169/J179 SIP R1.5.0 - Only Full path URLs are supported (relative paths are not supported).
## The Maximum size (pixels) is 320 x 240 (color depth 16 bit for J179) and JPG file type.
## 96x1 SIP R6.0 and later. Only Full path URLs are supported (relative paths are not supported).
## The models supported are: 9611G, 9621G and 9641G. The Maximum size (pixels) are: 217 x 130,
## 232 x 140 and 232 x 140 respectively with color depth 16 bit and JPG file type.
## H1xx SIP R1.0.1 and later. LOGOS defines list of administrator wallpapers.
## For best results, H175 Wallpapers resolution shall be 1280x800 with 24 bits color depth.
## The following file types are supported by H175: PNG, JPG (JPEG), GIF and BMP (GIF is presented without animation).
## Avaya Vantage Devices SIP R1.0.0.2 and later. LOGOS defines list of administrator wallpapers.
## For best results, Avaya Vantage Wallpapers resolution shall be 1280x800 with 24 bits color depth.
## The following file types are supported by Avaya Vantage: PNG, JPG (JPEG), GIF and BMP (GIF is presented without animation).
## Note: LOGOS is not supported by J100 SIP R2.0.0.0 and later. Please refer to BACKGROUND_IMAGE.
## SET LOGOS FIFAWorldCup=../fifa_logo.jpg
## SET LOGOS FIFAWorldCup=http://10.11.12.13/logo.jpg
## SET LOGOS FIFAWorldCup=http://logos.com/logo.jpg
##
```

Options Menu Display

```
## Determines whether Options & Settings menu is displayed
## on phone.
## 0 for No
## 1 for Yes
## Note: This parameter is also supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later.
## SET PROVIDE_OPTIONS_SCREEN 1
##
```

Network Info Menu Display

```
## Determines whether Network Information menu is displayed
## on phone.
## 0 for No
## 1 for Yes
## Note: This parameter is also supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later.
## SET PROVIDE_NETWORKINFO_SCREEN 1
##
```

Logout Enabled

```
## Determines whether user can log out from phone.
## 0 for No
## 1 for Yes
## SET PROVIDE_LOGOUT 1
## Note: This parameter is also supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later.
## Determines whether log out option is available or not in Avaya Menu options.
##
```

DISPLAY_SSL_VERSION - display version of OpenSSH/OpenSSL

```
## Value Operation
## 0 No display of OpenSSH/OpenSSL version (default)
## 1 Display of OpenSSH/OpenSSL version
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.0.0 and later
## SET DISPLAY_SSL_VERSION 1
```

CALL LOG SETTINGS

```
##
## Call Log Enabled
## Determines whether call logging and associated menus
## are available on the phone.
## 0 for No
## 1 for Yes
## Note: This parameter is also supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later and Avaya Vantage Basic
## Application SIP R1.0.0.1 and later.
## SET ENABLE_CALL_LOG 1
##
## Redial Enabled
## Determines whether redial softkey is available.
## 0 for No
## 1 for Yes
## Note: This parameter is also supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later and
## Avaya Vantage Basic Application SIP R1.0.0.0 and later.
## SET ENABLE_REDIAL 1
```

```

##
## Redial List Enabled
## Determines whether phone redials last number or
## displays list of recently dialed numbers.
## 0 for last number redial
## 1 user can select between last number redial and
## redial list
## Note: This parameter is also supported by J100 SIP R2.0.0.0 and later (J169/J179 only)
## SET ENABLE_REDIAL_LIST 1

##### CONTACTS SETTINGS #####
##
## Contacts Enabled
## Determines whether the contacts application and
## associated menus are available on the phone.
## 0 for No
## 1 for Yes
## Note: This parameter is also supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later and Avaya Vantage Basic
Application SIP R1.0.0.1 and later.
## Note: This parameter is also supported by H1xx R1.0.1 SIP and later, but it controls only
## the "Contacts" virtual button LED whether it is dimmed and pressing on it has no effect (ENABLE_CONTACTS==0) or
## whether "Contacts" virtual button LED is ON and pressing on it has effect (ENABLE_CONTACTS==1, default).
## SET ENABLE_CONTACTS 1

## CONTACT_NAME_FORMAT specifies how contact names are displayed.
## Value Operation
## 0 "Last Name, First Name" (Default)
## 1 "First Name Last Name"
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later
## SET CONTACT_NAME_FORMAT 0

##### COUNTRY AND DATE SETTINGS #####
##
## Call Progress Tone Country
## Country used for network call progress tones.
## For Argentina use keyword "Argentina"
## For Australia use keyword "Australia"
## For Brazil use keyword "Brazil"
## For Canada use keyword "USA"
## For France use keyword "France"
## For Germany use keyword "Germany"
## For Italy use keyword "Italy"
## For Ireland use keyword "Ireland"
## For Mexico use keyword "Mexico"
## For Spain use keyword "Spain"
## For United Kingdom use keyword "UK"
## For United States use keyword "USA"
##
## NOTE 1: For a complete list of supported countries, see your telephone's Administrators Guide.
## Note 2: Country names with spaces shall be enclosed in double quotes, as in:
## SET COUNTRY "Saudi Arabia"
## NOTE 3: This setting is also applicable for J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later. For J100
SIP R2.0.0.0 please use
## WLAN_COUNTRY for Wi-Fi Regulatory Domain configuration.
## Note 4: This parameter is supported by H1xx SIP R1.0 and later. For H1xx this parameter is used for country configuration for the
following:
## a. Call Progress Tones, b. cordless handset, c. Wi-Fi and d. default anti-flickering ("50" or "60" Hz).
## This parameter MUST be configured for cordless handset operation (only certain countries
## are supported with cordless handset. Refer to Administrator guide for the full list).
## The default of this parameter is "Undefined" which means:
## a. Call progress Tones for "USA", b. Cordless handset is disabled, c. Wi-Fi is configured as WorldWide and d. "60 Hz" anti-
flickering is used.
## Note 5: This parameter is supported by Avaya Vantage Devices SIP R1.0.0.0 and later. For Avaya Vantage Devices this parameter is
used for
## country configuration for Wi-Fi. The default of this parameter is "USA".
##
## SET COUNTRY USA

```

```

## Daylight Savings Time Mode
## Specifies daylight savings time setting for phone.
## 0 for no daylight saving time
## 1 for daylight savings activated (time set to DSTOFFSET)
## 2 for automatic daylight savings adjustment (as
## specified by DSTSTART and DSTSTOP)
## Note: This parameter is supported by H1xx SIP R1.0 only (TIMEZONE shall be used in R1.0.0.1 and later).
## Note: This parameter is also supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later.
## SET DAYLIGHT_SAVING_SETTING_MODE 2

##### PORT SETTINGS (SIP ONLY) #####
##
## UDP Minimum Port Value
## Specifies the lower limit of the UDP port range
## to be used by RTP/RTCP or SRTP/SRTCP connections.
## (1024 -65503).
## Note : This setting is also applicable for J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later,
## Avaya Vantage Basic Application SIP R1.0.0.0 and later and Avaya Equinox 3.1.2 and later.
## Note: For H1xx SIP R1.0 and later the first half of the range is used for audio
## and the second half for video.
## SET RTP_PORT_LOW 5004
##
## UDP Port Range
## Specifies the range or number of UDP ports
## available for RTP/RTCP or SRTP/SRTCP connections.
## This value is added to RTP_PORT_LOW to determine
## the upper limit of the UDP port range (32-64511).
## Note : This setting is also applicable for J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later,
## Avaya Vantage Basic Application SIP R1.0.0.0 and later and Avaya Equinox 3.1.2 and later.
## Note: For H1xx SIP R1.0 and later the first half of the range is used for audio
## and the second half for video.
## SET RTP_PORT_RANGE 40
##
## Signaling Port Minimum Value
## Specifies the minimum port value for SIP
## signaling.
## (1024 -65503).
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later - the default and minimum values are 5062.
## J169/J179 SIP R1.5.0 - the default and minimum values are 5062
## J129 SIP R1.0.0.0 (or R1.1.0.0) - the default is 1024
## 96xx SIP R2.0 and later
## 96x1 SIP R6.0 and later; Pre R7.1.1.0 the default is 1024. R7.1.1.0.0+ the default and minimum values are 5062.
## H1xx SIP R1.0 and later
## SET SIG_PORT_LOW 1024
##
## Signaling Port Range
## Specifies the range or number of SIP signaling
## ports. This value is added to SIG_PORT_LOW to
## determine the upper limit of the SIP signaling
## port range (32-64511).
## This parameter is supported by:
## J100 SIP R2.0.0.0 and later - the maximum value is 60473
## J169/J179 SIP R1.5.0 - the maximum value is 60473
## J129 SIP R1.0.0.0 (or R1.1.0.0) - the maximum value is 64511
## 96xx SIP R2.0 and later
## 96x1 SIP R6.0 and later; Pre R7.1.0.0 the maximum value is 64511. R7.1.1.0.0+ the maximum value is 60473.
## H1xx SIP R1.0 and later
## SET SIG_PORT_RANGE 64511

#####
##
## 96xx/96x1/H1xx/J129/J169/J179 SIP TELEPHONE SETTINGS
##
#####
## INGRESS_DTMF_VOL_LEVEL specifies the power level of tone, expressed in dBm0.

```

```

## The possible values are in the range of -20dBm to -7dBm.
## The default value is -12dBm.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0 and J100 SIP R2.0.0.0 and later
##   96xx SIP R2.0 and later
##   96x1 SIP R6.0 and later
##   H1xx SIP R1.0 and later
## SET INGRESS_DTMF_VOL_LEVEL -12

#####
##
## Conference transfer on primary appearance
## When CONF_TRANS_ON_PRIMARY_APPR is set to 1,
## conference and transfer setup will first attempt
## to use an idle primary call appearance even if
## initiated from a bridged call appearance.
## If an idle primary call appearance is not available,
## then an idle bridged call appearance will be used.
## Conference and transfer setup initiated from a bridged call
## appearance when no idle primary call appearance is available
## will next attempt to use an idle bridged call appearance of
## the same extension and if not available, an idle bridged call
## appearance of a different extension.
## Note: When CONF_TRANS_ON_PRIMARY_APPR is set to 1, AUTO_SELECT_ANY_IDLE_APPR is ignored.
##
## When CONF_TRANS_ON_PRIMARY_APPR is set to 0,
## conference and transfer setup initiated from a primary call
## appearance will first attempt to use an idle primary call appearance.
## If an idle primary call appearance is not available, it will use an idle
## bridged call appearance regardless of the setting of AUTO_SELECT_ANY_IDLE_APPR.
## Conference and transfer setup initiated from a bridged call appearance will attempt
## to use an idle bridged call appearance of the same extension.
## If an idle bridged call appearance of the same extension is not available
## and AUTO_SELECT_ANY_IDLE_APPR is set to 1, then conference and transfer
## setup will use any idle call appearance (primary or bridged).
## It will first attempt to find an idle primary call appearance and if not
## available will then attempt to find an idle bridged call appearance of a different extension.
## However, if AUTO_SELECT_ANY_IDLE_APPR is set to 0, transfer and conference setup
## initiated on a bridged call appearance will be denied if an idle bridged call appearance
## of the same extension is not available.
##
## The Default value of CONF_TRANS_ON_PRIMARY_APPR is 0.
## Note: These parameters are supported on SIP release R2.4.1 and later release of 96xx SIP telephones.
## Note: CONF_TRANS_ON_PRIMARY_APPR is supported by J100 SIP R2.0.0.0 and later (J169/J179 only).
##
## Auto Select any idle appearance
## When AUTO_SELECT_ANY_IDLE_APPR is active then any idle appearance is selected.
## When AUTO_SELECT_ANY_IDLE_APPR is set to 0 and CONF_TRANS_ON_PRIMARY_APPR is 0,
## then if no associated call appearance is selected,
## the conference or transfer operation will be denied.
## When AUTO_SELECT_ANY_IDLE_APPR is set to 1 and CONF_TRANS_ON_PRIMARY_APPR is 0,
## then if no associated call appearance is selected, the conference or transfer
## operation will be tried on any available call appearance (primary or bridged).
## This parameter is supported by:
##   96x0 SIP R2.4.1 and later releases
##   J100 SIP R2.0.0.0 and later (J169/J179 only).
## SET AUTO_SELECT_ANY_IDLE_APPR 0
##
## EXTEND_RINGTONE provides a way to customize ring tone files.
## This is a comma separated list of file names in xml format.
## The default value of this parameter is null.
## This parameter is supported by:
##   J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
##   96x0 SIP R2.4.1 and later releases
##   96x1 SIP R6.0 and later releases
## SET EXTEND_RINGTONE ""
##

```



```

##
## Dynamic Feature Set Discovery
## If the DISCOVER_AVAYA_ENVIRONMENT parameter value is 1, the phone discovers (determines)
## if that controller supports the AST feature set or not. The phone will send a SUBSCRIBE
## request to the active controller for the Feature Status Event Package (avaya-cm-feature-status).
## If the request succeeds, then the phone proceeds with PPM Synchronization.
## If the request is rejected, is proxied back to the phone or does not receive a response,
## the phone will assume that AST features are not available.
## If the parameter value is 0, the phone operates in a mode where AST features are not available.
## Note: This parameter is supported on R2.4.1 and later release of 96xx SIP telephones, H1xx SIP R1.0 and later
## and J129 SIP R1.0.0.0 (or R1.1.0.0) and J100 SIP R2.0.0.0 and later.
## For IP office and 3PCC environments this parameter shall be set to 0.
## SET DISCOVER_AVAYA_ENVIRONMENT 1
##
## Telephone number to call into the messaging system
## PSTN_VM_NUM is the "dialable" string is used to call into the messaging system
## (e.g. when pressing the Message Waiting button).
## Note: This parameter is supported on R2.4.1 and later release of 96xx SIP telephones, H1xx SIP R1.0 and later,
## Avaya Vantage Basic Application SIP R1.1.0.1 and later and J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later.
## PSTN_VM_NUM shall be used instead of MSGNUM in cases of IP Office environment, 3PCC SIP environment or when there is failover
## from Aura environment to a non-Aura server.
## SET PSTN_VM_NUM ""
##
## PSTN Access Prefix
## ENABLE_REMOVE_PSTN_ACCESS_PREFIX parameter allows telephone to
## perform digit manipulation during failure scenarios. This parameter
## allows removal of PSTN access prefix from the outgoing number.
## 0 - PSTN access prefix is retained in the outgoing number
## 1 - PSTN access prefix is stripped from the outgoing number.
## Note: This parameter is supported on R2.4.1 and later release of 96xx SIP telephones, H1xx SIP R1.0 and later
## and J129 SIP R1.0.0.0 (or R1.1.0.0) and J100 SIP R2.0.0.0 and later when the phone is failed over.
## This parameter is not supported in IP Office and 3PCC environments as there is no support for failover.
## SET ENABLE_REMOVE_PSTN_ACCESS_PREFIX 0
##
## Local Dial Area Code
## LOCAL_DIAL_AREA_CODE indicates whether user must dial area code for calls within same
## area code regions. when LOCAL_DIAL_AREA_CODE is enabled (1), the area code parameter (PHNLAC)
## should also be configured (ie. not the empty string).
## 0 - User don't need to dial area code.
## 1 - User need to dial area code.
## Note: This parameter is supported on R2.4.1 and later release of 96xx SIP telephones
## when the phone is failed over.
## Note: This parameter is supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later.
## SET LOCAL_DIAL_AREA_CODE 0
##
## Phone's Local Area Code
## When PHNLAC is set, it indicates the telephone's local area code, which along with
## the parameter LOCAL_DIAL_AREA_CODE, allows users to dial local numbers with more flexibility.
## PHNLAC is a string representing the local area code the telephone.
## Note: This parameter is supported on R2.4.1 and later release of 96xx SIP telephones
## when the phone is failed over.
## Note: This parameter is supported by J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later.
## SET PHNLAC ""
##
##### SIP USER CREDENTIALS SETTINGS #####
##
## SIP User Credentials settings
## Configure Username, Password and User ID to be used
## for SIP Registration. Usernames are often identical
## to User ID.
## FORCE_SIP_USERNAME replaces user field entered by user during Login
## FORCE_SIP_PASSWORD replaces password entered by user during Login
## FORCE_SIP_EXTENSION replaces User ID entered by user during Login
## If these are set, the user will not be prompted to Login on power cycle.
## Note: This parameter is supported by:
## J129 SIP R1.1.0.0, J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later
## 96x1 SIP R7.1.1.0 and later
## SET FORCE_SIP_USERNAME "7415"

```



```
## SET FORCE_SIP_PASSWORD "2222"
## SET FORCE_SIP_EXTENSION "741515"
##
## GET $MACADDR will request for the "MACADDR" file from the HTTP/HTTPS Server where "$MACADDR" which will be replaced by
the telephone's MAC address.
## Note: This parameter is supported by J129 SIP R1.1.0.0, J169/J179 R1.5.0, J100 SIP R2.0.0.0 and later and 96x1 SIP R7.1.1.0 and later
## GET $MACADDR.txt
```

License Agreements

License agreements are available at <https://support.avaya.com/Copyright>. Please select J100 Series IP Phones.

2018 Avaya Inc. All Rights Reserved.

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.