



## Avaya J100 Series IP Phone SIP Release 1.5.0.0 Readme

---

This file is the Readme document for the Avaya J100 Series IP Phone SIP Release 1.5.0.0 software (J100 SIP R1.5). This file describes the contents of the March 2018 release software distribution package.

Avaya J100 SIP R1.5 software is supported on the Avaya J169, J179 IP Phones used with Avaya Aura®. Avaya J100 SIP R1.5 software is also supported on the Avaya J169, J179 IP Phones used with Avaya IP Office™ in a Centralized Branch configuration. The Avaya J100 R1.5 software will not load or operate on any other models.

This is the first Software Release for J169 and J179, it does not supersede any other software release.

**IMPORTANT NOTE:** Avaya J100 SIP R1.5 is equivalent to Avaya 96x1 SIP R7.1.1.0 for feature functionality, however the J100 SIP R1.5 only runs on J169 and J179 hardware. No other phone can upgrade to or use J100 SIP R1.5.

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 J169 and J179 IP Phones using Avaya J100 SIP R1.5 software are supported on:

- 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, Avaya Aura® Presence Services 6.2.4) and associated service packs
- Avaya Aura® Platform 7.0.1.0 (Avaya Aura® Communication Manager 7.0.1.0, Avaya Aura® Session Manager 7.0.1.0, Avaya Aura® System Manager 7.0.1.0, Avaya Aura® Presence Services 7.0.1.0) and associated service packs
- Avaya Aura® Platform 7.1.0.0 (Avaya Aura® Communication Manager 7.1.0.0, Avaya Aura® Session Manager 7.1.0.0, Avaya Aura® System Manager 7.1.0.0, Avaya Aura® Presence Services 7.1.0.0) and associated service packs
- Avaya Aura® Platform 7.1.1.0 (Avaya Aura® Communication Manager 7.1.1.0, Avaya Aura® Session Manager 7.1.1.0, Avaya Aura® System Manager 7.1.1.0) and associated service packs
- Avaya Aura® Call Center Elite 6.3.6, 7.0.1.0, 7.1.0.0
- IP Office™ 11 and associated service packs when deployed in a Centralized Branch configuration

Avaya Aura® Platform 7.1.0.0 is the minimum requirement to support the following features:

- Support for dual-stack IPv4/IPv6

## **Features in SIP 1.5.0.0**

---

Avaya J100 SIP R1.5 supports all the features supported by SIP Release 7.1.1.0.

## Documentation for SIP 1.5.0.0

---

The following documentation has been provided for this release:

- [Installing and Administering J169/J179 IP Phone SIP](#)
- [Using Avaya J169/J179 IP Phones SIP](#)
- [Avaya J100 Series IP Phone Overview and Specifications](#)
- [Avaya J169/J179 IP Phone Quick Reference](#)
- [Using JBM24 Button Module](#)

These documents are available on <http://support.avaya.com> under "J100 Series IP Phones "  
-> "SIP 1.5.x" -> Documents

## SIP 1.5.0.0 (1.5.0.0.15) Package Content

---

The SIP 1.5.0.0 package (J100-IPT-SIP-R1\_5\_0\_0-121217.zip) contains all the files necessary to upgrade Avaya new or previously installed Avaya J169 or J179 IP Phones to the latest SIP 1.5.0.0 software.

- FW\_S\_J169\_R1\_5\_0\_0\_15.bin – The J169 SIP 1.5.0.0 application binary file.
- FW\_S\_J179\_R1\_5\_0\_0\_15.bin – The J179 SIP 1.5.0.0 application binary file.
- J100Supgrade.txt – The SIP 1.5.0.0 application upgrade file.
- Fifteen predefined language files for each Model (J169 and J179) plus Large English file for phone display:
  - Mlf\_J169Arabic.xml
  - Mlf\_J169BrazilianPortuguese.xml
  - Mlf\_J169CanadianFrench.xml
  - Mlf\_J169CastilianSpanish.xml
  - Mlf\_J169Chinese.xml
  - Mlf\_J169Dutch.xml
  - Mlf\_J169Englarge.xml
  - Mlf\_J169English.xml
  - Mlf\_J169German.xml
  - Mlf\_J169Hebrew.xml
  - Mlf\_J169Italian.xml
  - Mlf\_J169Japanese.xml
  - Mlf\_J169Korean.xml
  - Mlf\_J169LatinAmericanSpanish.xml
  - Mlf\_J169ParisianFrench.xml
  - Mlf\_J169Russian.xml
  - Mlf\_J179Arabic.xml
  - Mlf\_J179BrazilianPortuguese.xml
  - Mlf\_J179CanadianFrench.xml
  - Mlf\_J179CastilianSpanish.xml
  - Mlf\_J179Chinese.xml
  - Mlf\_J179Dutch.xml
  - Mlf\_J179Englarge.xml
  - Mlf\_J179English.xml
  - Mlf\_J179German.xml
  - Mlf\_J179Hebrew.xml
  - Mlf\_J179Italian.xml
  - Mlf\_J179Japanese.xml
  - Mlf\_J179Korean.xml
  - Mlf\_J179LatinAmericanSpanish.xml
  - Mlf\_J179ParisianFrench.xml
  - Mlf\_J179Russian.xml
- Eight extended Korean ring tone files:
  - KoreanRT1.xml
  - KoreanRT2.xml
  - KoreanRT3.xml
  - KoreanRT4.xml
  - KoreanRT5.xml
  - KoreanRT6.xml
  - KoreanRT7.xml
  - KoreanRT8.xml

- One certificate file:
  - av\_prca\_pem\_2033.txt – Avaya Product Root CA certificate with an expiration date of 2033
- Avaya-SparkIPTelephone-MIB.mib
- 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 SIP 1.5.0.0 software**

---

### **SLAMON – SLA Monitor**

SLA Monitor does not support J169 and J179 phones running J100 SIP R1.5. This will be supported in J100 SIP R2.0.

### **Limitations with IPv6**

J100 SIP R1.5 includes support for IPv6 interworking. The following are known limitations of the current implementation:

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

As a result of these limitations, J169 and J179 IP Phones will only be supported in a mixed IPv4/IPv6 environment.

### **SSH – Remote Access (ASG/EASG)**

J100 SIP R1.5 software contains an SSH server which is used by Avaya Services only for debugging purposes. The SSH server supports only Avaya Services Logins ("craft" and "sroot"). By enabling Avaya Services Logins, you are granting Avaya access to your system. This is required to maximize the performance and value of your Avaya support entitlements by allowing Avaya to resolve product issues in a timely manner. By disabling Avaya Services Logins, you are preventing Avaya access to your system. This is not recommended as it can impact Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Services Logins should not be disabled. The access to the SSH server is protected by EASG (new authentication algorithm).

## Support for SHA2-signed software files

As part of the security features in J100 SIP R1.5 software, the software files are signed using both SHA-1 and SHA-256 digital signatures. J100 SIP R1.5 software is capable of SHA-1 and SHA-256 digital signature verification.

## Removal of Avaya SIP Root CA Certificate

In J100 SIP R1.5, the Avaya SIP Root CA Certificate (av\_sipca\_pem\_2027.txt) is not included in the installation package.

## Support for OCSP

J100 SIP R1.5 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 R1.5 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.***

## 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 3<sup>rd</sup>-party vendors is undertaken through the Avaya [DevConnect](#) program.

## J169 IP Phone – Minimum Software Release

The J169 IP Phone must use J100 SIP R1.5.0.0 or later software. **Attempts to downgrade this model to other versions of software will be rejected.**

## J179 IP Phone – Minimum Software Release

The J179 IP Phone must use either J100 SIP R1.5.0.0 or later software. **Attempts to downgrade this model to lower versions of software will be rejected**

## Microsoft Exchange Integration using EWS

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

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

## Avaya Presence Services - Instant Messaging (IM) and Presence

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

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

Note: there must be no spaces in the certificate list

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

Avaya J100 SIP R1.5 supports Presence Communication Profiles which explicitly associates a user with an Avaya Aura® Presence Services (PS) server instance. If a Fully Qualified Domain Name (FQDN) is programmed via the Presence Communications Profile, the associated FQDN must be resolvable to the same IP address by both Avaya Aura® Session Manager (including via Local Host Name Resolution) and via Domain Name System (DNS) on the IP Phone. The IP address / FQDN received via this mechanism supersedes any PS IP address programmed in the 46xxsettings.txt file (via SET PRESENCE\_SERVER).

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

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

```
SET TLSSRVRID 0
```

2) If validation is required then settings file should have

```
SET TLSSRVRID 1 (this is the default value)
```

```
SET FQDN_IP_MAP "FQDN name=IP address"
```

### **Restriction on Busy Indicators on Button Modules:**

- A maximum of 3 button modules can be connected to the J169 or J179 IP Phones
- The J169 and J179 must be power cycled when connecting the first Button Module. This will automatically adjust the IEEE PoE setting to ensure enough power for the Button Modules
- The maximum combined number of busy indicators, team buttons and bridged appearances that can be configured on button modules is **48**.
- All button module lines can be configured as long as the restriction above is met.

### **Debug mode**

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

### **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. The use of Fully Qualified Domain Names (FQDN) is not supported. This applies to all sources of the SIP\_CONTROLLER\_LIST parameter which includes DHCP, LLDP, and the 46xxsettings.txt file

### **SRTP (Media Encryption)**

In order to correctly use SRTP, there are various components within the network that you must correctly configure. For J169 and J179 IP Phones to function properly with SRTP, you must configure the equivalent parameters in Communication Manager or System Manager. Avaya strongly recommends that the following three parameters on the J169 and J179 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 SIP R1.5 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.

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

## **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 R1.5 supports "Headset Profiles" to provide optimum performance for different brands of headsets. An up-to-date version of the profile <-> vendor cross reference can be found at <https://downloads.avaya.com/css/P8/documents/100173755>.

## **Avaya Session Border Controller for Enterprise**

For all IP 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 IP Phone SIP software.

## **Encryption – SHA2 and RSA 2048**

Avaya Deskphone SIP Release 1.5.0.0 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 Deskphone SIP Release 1.5.0.0.6 does not currently support the Avaya Diagnostic Server.

## **“Desk Phone” Mode and Lock**

Avaya one-X<sup>®</sup> 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 Phone. 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.

## **J169 and J179 - Aliasing**

Avaya Aura<sup>®</sup> Communication Manager does not provide native support of the J169 and J179 SIP IP Phone. The J169 and J179 IP Phones should be administered as a “9611SIP”.

## **Demo Certificates – Avaya Aura<sup>®</sup> Session Manager 6.3.8 and newer**



New installations of Avaya Aura<sup>®</sup> 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 Phones 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<sup>®</sup> Session Manager Release 6.3.8 or later preserves the demo Avaya certificates used on SIP and HTTPS (PPM) TLS connections. It is highly recommended to replace the demo Avaya certificates. Refer to the Session Manager Administrator Guide for more details.

## **Security Certificates – IP Address versus FQDN**

There is an industry movement towards the use of a FQDN (Fully Qualified Domain Name) instead of an IP address for the Subject Alternate Name or Subject Common Name for security certificates. Avaya J100 SIP R1.5 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.

## 802.1x – Authentication

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

- 1) Disable any 802.1x supplicant on the PC
- 2) Disable the 802.1x "pass-thru" mode on the phone.

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

## Interworking – TLS 1.2

J100 SIP R1.5 software includes EAP-TLS to support TLS 1.2 and includes cipher suites FIPS:!ADH:!DSS:-SSLv3:DHE-RSA-AES256-SHA:AES256-SHA:DHE-RSA-AES128-SHA:AES128-SHA.



J100 SIP R1.5 software 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.

## Unresolved issues in SIP 1.5.0.0.15

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
<b>User Interface</b>		
	SIP96X1-17503	IP Phone is not able display a name which has been configured with "@" as part of the name.
1-12671341066	SIP96X1-24119	ELD Rules not working. User is not able to dial 11 digit national calls from history.
	SIP96X1-23746	IP Phone 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".
	SIP96X1-24888	Config Server always displays HTTP port (port 80) although it is using HTTPS port (port 443)
	SIP96X1-29060	Transfer upon hang up does not work <b>Workaround:</b> 1 - press the Complete button or 2 - ENABLE_BLIND_TRANSFER set to '0'
<b>Audio</b>		
	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.
<b>Presence and Instant Messaging</b>		
	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". <b>Workaround: Log out and then back in.</b>
<b>Avaya SBCE – HA Failover</b>		
	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.
<b>Networking</b>		

External ID	Internal ID	Issue Description
	SIP96X1-17137	Phone sends wrong SIP Syslog message while it is rebooted remotely
<b>FIPS</b>		
	SIP96X1-23977	IP Phone 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 IP Phone does not display a "certificate rejected" message but does continue to use the original valid certificate.
<b>MLPP</b>		
	SIP96X1-24689	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. (Fixed in 2.0.0.0)
<b>SLA Monitor</b>		
	SIP96X1-27849	SLA Mon server cannot remote control to J179 phone (Fixed in 2.0.0.0)
<b>JBM24</b>		
	SIP96X1-29509	J179/J169 PoE Power calculations are not correct for JBM24 (Fixed in 2.0.0.0)

## Appendix 1 – Supported Hardware

---

J100 SIP Release 1.5.0.0 software is supported on the following models of IP Phones. All models ship pre-installed with SIP software and must be upgraded to SIP 1.5.0.0 GA as part of the installation process.

Comcode	Short Description	Model	Note
700513634	J169	J169D01A	Ships with SIP software.
700513569	J179	J179D02A	Ships with SIP 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	<a href="https://support.avaya.com/css/P8/documents/101033485">https://support.avaya.com/css/P8/documents/101033485</a>
1.1.0.0	1.0.0.0.15	Mar 2017	<a href="https://support.avaya.com/css/P8/documents/101037079">https://support.avaya.com/css/P8/documents/101037079</a>
1.1.0.1	1.0.0.1.3	Aug 2017	<a href="https://support.avaya.com/css/P8/documents/101042514">https://support.avaya.com/css/P8/documents/101042514</a>
1.5.0.0	1.5.0.0.15	Mar 2018	<a href="http://support.avaya.com/css/P8/documents/101047039">http://support.avaya.com/css/P8/documents/101047039</a>

## 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](https://support.avaya.com/downloads/download-details.action?contentId=C201773928555860_8&productId=P1661)

### New parameters.

```
#####  
##  
# PRODUCT_LINE_SETTINGS  
##  
#####  
  
IF $MODEL4 SEQ 9610 GOTO SETTINGS96X0  
IF $MODEL4 SEQ 9620 GOTO SETTINGS96X0  
IF $MODEL4 SEQ 9630 GOTO SETTINGS96X0  
IF $MODEL4 SEQ 9640 GOTO SETTINGS96X0  
IF $MODEL4 SEQ 9650 GOTO SETTINGS96X0  
IF $MODEL4 SEQ 9670 GOTO SETTINGS96X0  
IF $MODEL4 SEQ 9608 GOTO SETTINGS96X1  
IF $MODEL4 SEQ 9611 GOTO SETTINGS96X1  
IF $MODEL4 SEQ 9621 GOTO SETTINGS96X1  
IF $MODEL4 SEQ 9641 GOTO SETTINGS96X1  
IF $MODEL4 SEQ J129 GOTO SETTINGSJ100  
IF $MODEL4 SEQ J169 GOTO SETTINGSJ100  
IF $MODEL4 SEQ J179 GOTO SETTINGSJ100  
  
#####  
##  
# SETTINGSJ100  
##  
##### Add settings for J100 telephones below #####  
  
##### End of J100 SIP product line-specific settings #####  
GOTO PER_MODEL_SETTINGS  
  
#####  
##  
# PER_MODEL_SETTINGS  
##  
#####  
  
IF $MODEL4 SEQ 9610 GOTO SETTINGS9610  
IF $MODEL4 SEQ 9620 GOTO SETTINGS9620  
IF $MODEL4 SEQ 9630 GOTO SETTINGS9630  
IF $MODEL4 SEQ 9640 GOTO SETTINGS9640  
IF $MODEL4 SEQ 9650 GOTO SETTINGS9650  
IF $MODEL4 SEQ 9670 GOTO SETTINGS9670  
IF $MODEL4 SEQ 9601 GOTO SETTINGS9601  
IF $MODEL4 SEQ 9608 GOTO SETTINGS9608  
IF $MODEL4 SEQ 9611 GOTO SETTINGS9611  
IF $MODEL4 SEQ 9621 GOTO SETTINGS9621  
IF $MODEL4 SEQ 9641 GOTO SETTINGS9641  
IF $MODEL4 SEQ H175 GOTO SETTINGSH175  
IF $MODEL4 SEQ J129 GOTO SETTINGSJ129  
IF $MODEL4 SEQ J169 GOTO SETTINGSJ169  
IF $MODEL4 SEQ J179 GOTO SETTINGSJ179  
IF $MODEL4 SEQ K165 GOTO SETTINGSK165  
IF $MODEL4 SEQ K175 GOTO SETTINGSK175  
GOTO GROUP_SETTINGS  
  
#####  
##  
# SETTINGSJ129
```

```
##
##### Add settings for J129 SIP phones #####
##
## AUDIOSTHS specifies the level of sidetone in the handset. The sidetone level adjustment
## provided by the AUDIOSTHS parameter is applicable to both wired and DECT handsets.
## Value Operation
## 0 NORMAL level for most users (default)
## 1 three levels softer than NORMAL
## 2 OFF (inaudible)
## 3 one level softer than NORMAL
## 4 two levels softer than NORMAL
## 5 four levels softer than NORMAL
## 6 five levels softer than NORMAL
## 7 six levels softer than NORMAL
## 8 one level louder than NORMAL
## 9 two levels louder than NORMAL
## This parameter is supported by:
## J129 SIP R1.0.0.0 and later
## SET AUDIOSTHS 1
##
##### End of J129 SIP model-specific settings #####
GOTO GROUP_SETTINGS
```

```
# SETTINGSJ169
##
##### Add settings for J169 telephones below #####
##
## AUDIOSTHS specifies the level of sidetone in the handset.
## Value Operation
## 0 NORMAL level for most users (default)
## 1 three levels softer than NORMAL
## 2 OFF (inaudible)
## 3 one level softer than NORMAL
## 4 two levels softer than NORMAL
## 5 four levels softer than NORMAL
## 6 five levels softer than NORMAL
## 7 six levels softer than NORMAL
## 8 one level louder than NORMAL
## 9 two levels louder than NORMAL
## SET AUDIOSTHS 1
##
## AUDIOSTHD specifies the level of sidetone in the headset.
## Value Operation
## 0 NORMAL level for most users (default)
## 1 three levels softer than NORMAL
## 2 OFF (inaudible)
## 3 one level softer than NORMAL
## 4 two levels softer than NORMAL
## 5 four levels softer than NORMAL
## 6 five levels softer than NORMAL
## 7 six levels softer than NORMAL
## 8 one level louder than NORMAL
## 9 two levels louder than NORMAL
## SET AUDIOSTHD 1
##
##### End of J169 model-specific settings #####
GOTO GROUP_SETTINGS
```

```
# SETTINGSJ179
##
##### Add settings for J179 telephones below #####
##
## AUDIOSTHS specifies the level of sidetone in the handset.
## Value Operation
## 0 NORMAL level for most users (default)
## 1 three levels softer than NORMAL
## 2 OFF (inaudible)
## 3 one level softer than NORMAL
```

```
## 4 two levels softer than NORMAL
## 5 four levels softer than NORMAL
## 6 five levels softer than NORMAL
## 7 six levels softer than NORMAL
## 8 one level louder than NORMAL
## 9 two levels louder than NORMAL
## SET AUDIOSTHS 1
##
## AUDIOSTHD specifies the level of sidetone in the headset.
## Value Operation
## 0 NORMAL level for most users (default)
## 1 three levels softer than NORMAL
## 2 OFF (inaudible)
## 3 one level softer than NORMAL
## 4 two levels softer than NORMAL
## 5 four levels softer than NORMAL
## 6 five levels softer than NORMAL
## 7 six levels softer than NORMAL
## 8 one level louder than NORMAL
## 9 two levels louder than NORMAL
## SET AUDIOSTHD 1
##
##### End of J179 model-specific settings #####
GOTO GROUP_SETTINGS
```

## 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:
## 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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later
## 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 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:
## J169/J179 SIP R1.5.0
## 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 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:
## J169/J179 SIP R1.5.0
## 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 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:
## 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.
## J169/J179 SIP R1.5.0
## 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, 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 and later; 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:
## Avaya Vantage Devices SIP R1.1.0.0 and later for K165/K175 models with embedded Ethernet switch
## J169/J179 SIP R1.5.0
## 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
## 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
## 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:
## Avaya Vantage Devices SIP R1.1.0.0 and later for K165/K175 models with embedded Ethernet switch
## J169/J179 SIP R1.5.0
## 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:
## 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)
## J169/J179 SIP R1.5.0
## 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
##
## DSCPVID specifies the layer 3 Differentiated Services (DiffServ) Code Point
## for video frames generated by the telephone.
## Valid values are 0 through 63; the default value is 34.
## This parameter is supported by:
## Avaya Vantage Basic Application SIP R1.1.0.1 and later; used in IP office environment only (for Aura environment
## DSCPVID is taken from PPM and configured using SMGR)
## J169/J179 SIP R1.5.0
## 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 DSCPVID 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:
## 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)
## J169/J179 SIP R1.5.0
## 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 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
## 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
## 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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later
## 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 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 - 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 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:
##     J169/J179 SIP R1.5.0
##     Avaya Vantage Devices SIP R1.0.0.0 and later
##     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 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:
##     J169/J179 SIP R1.5.0
##     Avaya Vantage Devices SIP R1.0.0.0 and later
##     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 DOMAIN mycompany.com
##

##### SERVER SETTINGS (SIP) #####
## Note: Third party SIP call controllers (3PCC) support is only provided by J129 SIP R1.1.0.0 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:
##     J169/J179 SIP R1.5.0
##     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:
##     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
## 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]"
##

## 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:
## Avaya Vantage Basic Application SIP R1.1.0.1 and later
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 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
##

##
## 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:
## J169/J179 SIP R1.5.0

```

```

##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 and later; for IP office and 3PCC environments this parameter shall be set to 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
##

##### TIME SETTINGS (SIP ONLY) #####
##

## SNTPSRVR 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:
##      J169/J179 SIP R1.5.0
##      Avaya Vantage Devices SIP R1.0.0.0 and later
##      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 SNTPSRVR 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:
##      J169/J179 SIP R1.5.0
##      96x1 SIP R7.1.0.0 and later
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      Avaya Vantage Basic Application SIP R1.1.0.0 and later
##      J169/J179 SIP R1.5.0; valid values are 30 to 86400; the default value is 900.

```

```

##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:

```

```

##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0 (default value is 16)
##      J129 SIP R1.0.0.0 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:
##      J169/J179 SIP R1.5.0; the default value is 32.
##      J129 SIP R1.0.0.0 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 - 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:
##     J169/J179 SIP R1.5.0
##     J129 SIP R1.0.0.0 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:
##     J169/J179 SIP R1.5.0
##     J129 SIP R1.0.0.0 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:
##     J169/J179 SIP R1.5.0
##     J129 SIP R1.0.0.0 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
##
##
## 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:
##     J169/J179 SIP R1.5.0
##     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:
##     J169/J179 SIP R1.5.0
##     Avaya Equinox 3.1.2 and later
##     J129 SIP R1.0.0.0 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 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:
## J169/J179 SIP R1.5.0 (default is 1)
## J129 SIP R1.0.0.0 and later (default is 1); For IP office and 3PCC environments this parameter shall be set to 0 as presence is
not supported.
## 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
##
## PRESENCE_SERVER specifies the address of the Presence server.
## Zero or one IP address in dotted decimal,
## optionally followed by a colon and a TCP port number.
## The default value is null ("").
## Note: Starting with 96x1 R6.5 SIP, if the phone is deployed with Aura Platform 6.2 FP4 and later,
## the value of this parameter is used from PPM and not from the settings file.
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 96x1 SIP R6.2 and later
## 96x0 SIP R2.6.6 and later
## H1xx SIP R1.0 and later; this parameter is not supported in IP Office environment as presence is not supported.
## SET PRESENCE_SERVER 192.168.0.5:8090
##
## 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:
## J169/J179 SIP R1.5.0 (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
##

##### INSTANT MESSAGING SETTINGS (SIP ONLY) #####
##
## INSTANT_MSG_ENABLED specifies whether Instant Messaging will be enabled or disabled.
## Value Operation
## 0 Disabled
## 1 Enabled (default)
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 96x1 SIP R6.2 and later
## SET INSTANT_MSG_ENABLED 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
## 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
## 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
## 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
## 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
## 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
## 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
## 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
## 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
##      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
##      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
##
## EXCHANGE_SERVER_SECURE_MODE specifies whether to use HTTPS to contact Exchange servers.
## Value Operation
## 0 use HTTP
## 1 use HTTPS (default)
## This parameter is supported by:
##      J169/J179 SIP R1.5.0
##      96x1 SIP R6.3 and later.
##      H1xx SIP R1.0 and later
## SET EXCHANGE_SERVER_SECURE_MODE 0
##
## EXCHANGE_SERVER_MODE specifies the protocol(s) to be used to contact Exchange servers.
## Value Operation
## 1 use WebDAV
## 2 use Exchange Web Services (EWS)
## 3 try EWS first, if that fails, try WebDAV (default)
## This parameter is supported by:
##      J169/J179 SIP R1.5.0
##      96x1 SIP R6.3 and later.
## SET EXCHANGE_SERVER_MODE 1
##
## 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
##      96x1 SIP R6.2 and later
##      96x0 SIP R2.0 through R2.4 only
## SET PROVIDE_EXCHANGE_CONTACTS 0
##
##
## USE_EXCHANGE_CALENDAR specifies whether calendar data will be retrieved from Microsoft Exchange.
## Value Operation
## 0 Disabled (default)
## 1 Enabled
## This parameter is supported by:
##      J169/J179 SIP R1.5.0
##      96x1 SIP R6.0.x only (set only by user option in R6.2 and later)
##      96x0 SIP R2.5 and later
## SET USE_EXCHANGE_CALENDAR 1
##
## 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:
##      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
## 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
## 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
## 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
## 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
## 96x1 SIP R6.0 and later
## 96x0 SIP R2.5 and later
## SET EXCHANGE_SNOOZE_TIME 4
##
## 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; 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
## 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 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
##
## AUTO_UNMUTE specifies whether the call will be unmuted on a transducer changing. This applies to all calls.
## Value Operation
## 0 Disabled (default)
## 1 Enabled
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 96x1 SIP R7.1.0.0 and later
##
## 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 and later; not applicable for 3PCC environment
## 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 and later
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R2.6 and later
## SET 100REL_SUPPORT 1
##
## DISPLAY_NAME_NUMBER specifies whether the name and/or number will be displayed for
## incoming calls, and if both are displayed, the order in which they are displayed.
## Value Operation
## 0: display calling party name only
## 1: display calling party name followed by calling party number
## 2: display calling party number only
## 3: display calling party number followed by calling party name
## This parameter is supported by:
## J169/J179 SIP R1.5.0; valid values 0 through 3; the default value is 0.
## 96x1 SIP R6.2 and later; valid values 0 through 3; the default value is 0.
## 96x1 SIP R6.0.x; valid values 0 through 1; the default value is 0.
## 96x0 SIP R2.6.5 and later; valid values 0 through 3; the default value is 0.
## 96x0 SIP R2.0 through R2.6.4; valid values 0 through 1; the default value is 0.
## SET DISPLAY_NAME_NUMBER 0
##
## HOTLINE specifies zero or one hotline number.
## Valid values can contain up to 30 dialable characters (0-9, *, #).
## The default value is null ("").
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 96x1 SIP R6.2 and later
## SET HOTLINE ""
##
## 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 and later
## 96x1 SIP R6.2 and later
## H1xx SIP R1.0 and later
## SET PLAY_TONE_UNTIL_RTP 0
##
## PLUS_ONE specifies whether pressing the 1 key during dialing will alternate between 1 and +.
## Value Operation
## 0 1 key only dials 1 (default).
## 1 1 key alternates between 1 and +.
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 96x1 SIP R6.2 and later
## SET PLUS_ONE 1
##
## 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
## 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 and later
## 96x1 SIP R6.2 and later
## H1xx SIP R1.0 and later
## SET LOCALLY_ENFORCE_PRIVACY_HEADER 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
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later
## J129 SIP R1.0.0.0 and later
## 96x1 SIP R6.2 and later
## H1xx SIP R1.0 and later
## 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:
## J169/J179 SIP R1.5.0
## 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
## 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
## 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
## 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
## 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
## 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:
## J169/J179 SIP R1.5
## Avaya Vantage Devices SIP R1.0.0.0 and later
## J129 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:
## J169/J179 SIP R1.5
## Avaya Vantage Devices SIP R1.0.0.0 and later
## J129 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:

```

```
## Avaya Vantage Devices SIP R1.1.0.1 and later for IP Office Environment only
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 and later
## 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
##
```

```
##### 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 and later
## 96x1 SIP R6.2 and later
## SET ENABLE_SHOW_EMERG_SK_UNREG 1
##
```

```
##### CALL LOG SETTINGS #####
##
## CLDISPCONTENT specifies whether the name, the number, or both will be displayed for Call Log entries.
## Value Operation
## 0 Both the name and the number will be displayed
## 1 Only the name will be displayed (default)
## 2 Only the number will be displayed
## This parameter is supported by:
## J169/J179 SIP R1.5.0 (only supports values of 0 or 1)
## 96x1 H.323 R6.0 and up to R6.6.3 (excluded) (only supports values of 0 or 1)
## 96x1 H.323 R6.6.3 and later
## 96x1 SIP R6.0 and later (only supports values of 0 or 1)
## 96x0 H.323 R3.2 and later
## SET CLDISPCONTENT 0
##
## 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
## 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 (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
## 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
## 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
## 96x1 SIP R6.2 and later
## SET ENTRYNAME 1
##
## BUTTON_MAPPINGS specifies a list of Button=Status pairs that change the operation
## of some of the buttons on the telephone.
## Button=Status pairs are separated by commas without any intervening spaces.
## Valid Button values are "Forward", "Speaker", "Hookswitch", and "Headset".
## Valid Status values are "na" and "cc-release".
## Value Operation
## na The corresponding button will be disabled.
## cc-release The button will invoke the cc-release feature.
## If the value of BUTTON_MAPPINGS is null (the default), all buttons will operate normally.
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 96x1 SIP R6.2 and later
## SET BUTTON_MAPPINGS Forward=na,Speaker=cc-release,Hookswitch=na,Headset=na
##

```

```

## 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
##   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
##   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
##   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
##   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:
##   J169/J179 SIP R1.5.0
##   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.).
##   J129 SIP R1.0.0.0 and later
##   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:
## J169/J179 SIP R1.5.0
## 96x1 SIP 7.1.0.0 and later
## SET MAX_TRUSTCERTS 8

## TLSSRRVRID 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:
## J169/J179 SIP R1.5.0
## 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
## J129 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
## TLSSRRVRID is not supported by 96x1 H.323 phones and instead
## TLSSRRVRVERIFYID is supported (see below)
## SET TLSSRRVRID 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 if 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:
## J169/J179 SIP R1.5.0
## 96x1 SIP R7.1.0.0 and later
## J129 SIP R1.0.0.0 and later (IPv6 is not yet supported)
## 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:
##   J169/J179 SIP R1.5.0
##   96x1 SIP R7.1.0.0 and later
##   J129 SIP R1.0.0.0 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:
##   J169/J179 SIP R1.5.0
##   96x1 SIP R7.1.0.0 and later
##   Avaya Vantage Devices SIP R1.0.0.0 and later
##   J129 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:
##   J169/J179 SIP R1.5.0
##   96x1 SIP R7.1.0.0 and later
##   Avaya Vantage Devices SIP R1.0.0.0 and later
##   J129 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:
##   J169/J179 SIP R1.5.0
##   Avaya Vantage Devices SIP R1.0.0.0 and later; Not used by Avaya Vantage Open application.
##   J129 SIP R1.0.0.0 and later
##   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:
##   J169/J179 SIP R1.5.0
##   Avaya Vantage Devices SIP R1.0.0.0 and later; HTTPPROXY is NOT supported for SCEP, but for Android HTTP based applications.
##   J129 SIP R1.0.0.0 and later
##   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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later; HTTPPROXY is NOT supported for SCEP, but for Android HTTP based applications.
## J129 SIP R1.0.0.0 and later
## 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 - 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.
## J129 SIP R1.0.0.0 up to R1.1.0.0 (excluded) - the URL can be only http; R1.1.0.0 and later - the URL can be https or http.
## 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://certsrv.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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later; Avaya Vantage Open application does not use identity certificate.
## J129 SIP R1.0.0.0 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
## 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 "/" 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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later; Avaya Vantage Open application does not use identity certificate.
## J129 SIP R1.0.0.0 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 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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later; Avaya Vantage Open application does not use identity certificate.
## J129 SIP R1.0.0.0 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 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:
## J169/J179 SIP R1.5.0 - only "2048" is supported
## Avaya Vantage Devices SIP R1.0.0.0 and later; only value "2048" is supported.
## J129 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 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:
## 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.
## J129 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.
## 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:
## 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.
## J129 SIP R1.0.0.0 and later
## 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:
## J169/J179 SIP R1.5.0
## 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.
## J129 SIP R1.0.0.0 and later
## 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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later
## 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 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:
## Avaya Vantage Devices SIP R1.1.0.0 and later for K165/K175 models with embedded Ethernet switch
## J169/J179 SIP R1.5.0
## 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
## 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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later
## J129 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
## 96x1 SIP 7.1.0.0 and later
## 96x1 H.323 R6.6 and later
## SET FIPS_ENABLED 1
##
##### OCS (Online Certificate Status Protocol) SETTINGS #####
##
## OCS_ENABLED specifies whether OCS will be used to check revocation status of certificates.
## Value Operation
## 0 OCS is disabled (default)
## 1 OCS is enabled. OCS 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:
## J169/J179 SIP R1.5.0
## 96x1 SIP R7.1.0.0 and later
## J129 SIP R1.0.0.0 and later
## 96x1 H.323 R6.6 and later
## SET OCS_ENABLED 1
##
## OCS_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:
## J169/J179 SIP R1.5.0
## 96x1 SIP R7.1.0.0 and later
## J129 SIP R1.0.0.0 and later
## 96x1 H.323 R6.6 and later
## SET OCS_ACCEPT_UNK 1
##
## OCS_NONCE specifies whether a nonce will be included in OCS requests and expected in OCS responses.
## Value Operation
## 0 Nonce is NOT added to OCS packets
## 1 Nonce is added to OCS packets (Default)
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 96x1 SIP R7.1.0.0 and later
## J129 SIP R1.0.0.0 and later
## 96x1 H.323 R6.6 and later
## SET OCS_NONCE 1
##
## OCS_URI specifies the URI of an OCS 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:
## J169/J179 SIP R1.5.0
## 96x1 SIP R7.1.0.0 and later
## J129 SIP R1.0.0.0 and later
## 96x1 H.323 R6.6 and later
## SET OCS_URI http://clients1.google.com/ocs
##
## OCS_URI_PREF specifies the preferred URI to use for OCS requests if more than one is available.
## Value Operation
## 1 Use the OCS_URI first and then the OCS field of the Authority Information Access (AIA) extension
## of the certificate being checked (Default)
## 2 Use the OCS field of the Authority Information Access (AIA) extension of the
## certificate being checked first and then OCS_URI
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 96x1 SIP R7.1.0.0 and later
## J129 SIP R1.0.0.0 and later
## 96x1 H.323 R6.6 and later
## SET OCS_URI_PREF 0
##
## OCS_TRUSTCERTS specifies list of OCS trusted certificates which are used as

```

```

## OCSF signing authority for the certificate that its revocation status is being checked.
## This is needed in case the OCSF 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:
## J169/J179 SIP R1.5.0
## 96x1 SIP R7.1.0.0 and later
## J129 SIP R1.0.0.0 and later
## 96x1 H.323 R6.6 and later
## SET OCSF_TRUSTCERTS ocsf.cer
##
## OCSF_HASH_ALGORITHM specifies the hashing algorithm for OCSF request.
## Value Operation
## 0 SHA-1 (default)
## 1 SHA-256
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 96x1 SIP 7.1.0.0 and later
## J129 SIP R1.0.0.0 and later
## SET OCSF_HASH_ALGORITHM 1
##
## OCSF_USE_CACHE specifies if OCSF caching is used.
## Value Operation
## 0 Do not to use OCSF caching. Always check with OCSF responder.
## 1 Use OCSF cache caching (default).
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 96x1 SIP 7.1.0.0 and later
## J129 SIP R1.0.0.0 and later
## SET OCSF_USE_CACHE 1
##
## OCSF_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 OCSF response cache expiry uses nextUpdate value in OCSF response message. Only if nextUpdate is not present will the
OCSF_CACHE_EXPIRY parameter value be used.
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 96x1 SIP R7.1.0.0 and later
## J129 SIP R1.0.0.0 and later
## SET OCSF_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
## 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
##
## HOMEIDLETIME specifies the number of minutes of idle time after which the Home screen will be displayed.
## A value of 0 means that the Home screen will not be displayed automatically when the phone is idle.
## This parameter is supported by:
## 9621 and 9641 H.323 R6.0 and later (valid values are 0 through 30; the default value is 10)
## 9621 and 9641 SIP R6.0 and later (valid values are 0 through 30; the default value is 10)
## 9670 H.323 R2.0 and later (valid values are 5 through 30; the default value is 10)
## J129 R1.0.0.0 and later (valid values are 0 through 30; the default value is 10)
## Note: The parameter is not supported by J179/J169 SIP phones.

```

```

## SET HOMEIDLETIME 5
##
## 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) or LOGOS and CURRENT_LOGO (for SIP)
## parameter, 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:
## J169/J179 SIP R1.5.0
## 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, 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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later; Please note that ENABLE_PHONE_LOCK is used as enable/disable
## of lock screen.
## J129 SIP R1.0.0.0 and later; Please note that on J129 the Lock option appears in the main menu. There is no Lock softkey or feature
## button.
## 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:
## 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.
## J129 SIP R1.0.0.0 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.
## 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:
## J169/J179 SIP R1.5.0
## 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 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:
## J169/J179 SIP R1.5.0
## 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 ENABLE_G711U 0
##
## ENABLE_G722 specifies whether the G.722 codec is enabled.
## Value Operation
## 0 Disabled
## 1 Enabled
## This parameter is supported by:
## J169/J179 SIP R1.5.0; the default value is 1.
## J129 SIP R1.0.0.0 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:
## J169/J179 SIP R1.5.0
## 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; 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 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:
## J169/J179 SIP R1.5.0
## 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 ENABLE_G729 0
##
##
## 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:
## J169/J179 SIP R1.5.0
## 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 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:
## J169/J179 SIP R1.5.0
## Avaya Equinox 3.1.2 and later
## J129 SIP R1.0.0.0 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.
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 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:

```

```

## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 and later
## 96x1 SIP R6.2 and later
## 96x0 SIP R2.6.5 and later.
## SET MATCHTYPE 0
##

##
## USE_QUAD_ZEROES_FOR_HOLD specifies how Hold will be signaled in SDP.
## Value Operation
## 0 "a=directional attributes" will be used (default)
## 1 "c=0.0.0.0" will be used
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 96x1 SIP R6.0 and later
## H1xx SIP R1.0 and later
## 96x0 SIP R2.0 and later
## SET USE_QUAD_ZEROES_FOR_HOLD 1
##
##### 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
## 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:
## J169/J179 SIP R1.5.0 (values 1-5 only)
## J129 SIP R1.0.0.0 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:
##     Avaya Vantage Devices SIP R1.1.0.0 and later for K165/K175 models with embedded Ethernet switch (values 0-1 only)
##     J169/J179 SIP R1.5.0 (values 0-5 only)
##     J129 SIP R1.0.0.0 and later (values 0-5 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:
##     Avaya Vantage Devices SIP R1.1.0.0 and later for K165/K175 models with embedded Ethernet switch
##     J169/J179 SIP R1.5.0
##     J129 SIP R1.0.0.0 and later
##     H1xx SIP R1.0 and later
##     96x1 H.323 R6.3 and later
##     96x1 SIP R6.3 and later
## SET PHY2_AUTOMDIX_ENABLED 1
##

##### 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:
##     J169/J179 SIP R1.5.0
##     J129 SIP R1.0.0.0 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:
##     J169/J179 SIP R1.5.0 (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)
##     J129 SIP R1.0.0.0 and later (must contain at least 4 digits else default value 27238 is used)
##     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:
## J169/J179 SIP R1.5.0
## 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 "".
## J129 SIP R1.0.0.0 and later
## 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:
## J169/J179 SIP R1.5.0
## 96x1 SIP R7.1.0.0 and later
## J129 SIP R1.0.0.0 and later
## SET ADMIN_LOGIN_ATTEMPT_ALLOWED 11
##
## ADMIN_LOGIN_LOCKED_TIME specifies the time in minutes that local (craft) procedures are locked once the
## number of failed attempts for entering the access code (PROCPSWD or ADMIN_PASSWORD) is reached.
## Valid values 5 min to 1440 min, default 10 min.
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 96x1 SIP R7.1.0.0 and later
## J129 SIP R1.0.0.0 and later
## SET ADMIN_LOGIN_LOCKED_TIME 2

##### 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later; the default is 1.
## J129 SIP R1.0.0.0 and later
## 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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later
## J129 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:

```

```

## J169/J179 SIP R1.5.0
## 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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later; the default is "ALL" which implies all categories.
## J129 SIP R1.0.0.0 and later
## 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
## 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
## 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 impacts 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:
## J169/J179 SIP R1.5.0 ("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)
## J129 SIP R1.1.0.0 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 up to 7.1.0.0 (not included) is 0 (disabled). The default value for 96x1 SIP R7.1.0.0 and later is 2.
## The default of B189 is 0 (disabled).
## This parameter is supported by:
## 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)
## J129 SIP R1.0.0.0 and later (values 0-2), the default 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), value 2 is added in R7.1.0.0 and later.
## 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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later
## J129 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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 and later
## J129 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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 (build 2304) and later
## 96x1 SIP 7.1.0.0 and later
## J129 SIP R1.1.0.0 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:
## J169/J179 SIP R1.5.0
## Avaya Vantage Devices SIP R1.0.0.0 (build 2304) and later

```

```

## 96x1 SIP 7.1.0.0 and later
## J129 SIP R1.1.0.0 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:
## J169/J179 SIP R1.5.0
## 96x1 SIP 7.1.0.0 and later
## J129 SIP R1.1.0.0 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:
## J169/J179 SIP R1.5.0
## 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.
## J129 SIP R1.0.0.0 and later
## 96x1 SIP R7.0.1.0 and later releases (hardware version 3 and up).
## 96x1 H.323 R6.6.2 and later releases (hardware version 3 and up).
## SET AUTHCTRLSTAT 1
##

##### 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 and later,
## 96x1 SIP R6.0 and later, 96x1/B189 H.323 6.6 and later, H1xx SIP R1.0 and later, J169/J179 SIP R1.5.0)
## 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.
## J169/J179 SIP R1.5.0
## Avaya Equinox 3.1.2 and later; default is "".
## Avaya Vantage Basic Application SIP R1.0.0.1 and later; default is "".
## 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
## 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.
## J169/J179 SIP R1.5.0
## Avaya Equinox 3.1.2 and later; default is "".
## Avaya Vantage Basic Application SIP R1.0.0.1 and later; default is "".
## 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
## 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:
## J169/J179 SIP R1.5.0
## Avaya Equinox 3.1.2 and later; default is "".
## Avaya Vantage Basic Application SIP R1.0.0.1 and later; default is "".
## 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
## 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:
## J169/J179 SIP R1.5.0
## Avaya Equinox 3.1.2 and later; default is "".
## Avaya Vantage Basic Application SIP R1.0.0.1 and later; default is "".
## 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
## 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:
## J169/J179 SIP R1.5.0
## Avaya Equinox 3.1.2 and later; default is "".
## Avaya Vantage Basic Application SIP R1.0.0.1 and later; default is "".
## 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
## 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:

```

```

## J169/J179 SIP R1.5.0
## Avaya Equinox 3.1.2 and later; default is "".
## Avaya Vantage Basic Application SIP R1.0.0.1 and later; default is "".
## 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
## 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
## 96x1 SIP R7.0.1.2 and later.
##
## SET ELD_SYSNUM 1

##### 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:
## Avaya Vantage Devices SIP R1.1.0.0 and later
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 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
## 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
## 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
## 96x1 SIP R6.3 and later.

```

```

## SET RINGTONES_UPDATE 1
##
## PROVIDE_CF_RINGTONE specifies whether the call forward ringtone option is provided to the user.
## Value Operation
## 0 the call forward ringtone option is not provided (default)
## 1 the call forward ringtone option is provided
## This parameter is supported by:
## J169/J179 SIP R1.5.0
## 96x1 SIP R6.3 and later.
## SET PROVIDE_CF_RINGTONE 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/J129 SIP models in Avaya Aura
## environments, this parameter is set via the PPM server.
## Note : This setting is supported by J169/J179 SIP R1.5.0, H1xx SIP R1.0 and later and J129 SIP R1.0.0.0 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 J169/J179 SIP R1.5.0, 96xx SIP telephones and J129 SIP telephones in non-Avaya environments.
## For 96xx/J129 SIP
## models and J169/J179 SIP R1.5.0 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 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/J129 SIP telephones.
## Note : This setting is supported by J129 SIP R1.0.0.0 and later and J169/J179 SIP R1.5.0
## for non-Aura environment (For example: IP Office, etc).
## SET RTCPMONPERIOD 5

#####
##
## 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
## 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  
## 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 (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  
## 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
## 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
## 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:
## J169/J179 SIP R1.5.0
## 96x1 SIP R7.1.0.0 and later
## Example:
## SET IPV6DADXMITS 1
##
#####
##
## 96xx, J129, H1xx SIP SETTINGS
## Settings applicable only to 96xx, J129 telephone,
## J169/J179 SIP R1.5.0 models 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 and J129 SIP.
## 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:
## J169/J179 SIP R1.5.0
## J129 SIP R1.0.0.0 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, J169/J179 SIP R1.5.0, H1xx SIP R1.0.1 and later and J129 SIP R1.0.0.0 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 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:
##     J169/J179 SIP R1.5.0
##     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.
##     J129 SIP R1.0.0.0 and later
##     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.
## This parameter is supported by:
##     J169/J179 SIP R1.5.0
##     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
##     J129 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

##### 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:
##   J169/J179 SIP R1.5.0
##   J129 SIP R1.1.0.0 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 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.