Avaya J100 Series SIP Release 4.0.0.0 Readme

This file is the Readme for the Avaya J100 Series SIP Release 4.0.0.0 software (J100 SIP 4.0.0.0). This file describes the contents of the December 2018 (**4.0.0.0.21**) release software distribution package.

J100 SIP 4.0.0.0 software is supported on the Avaya J129, J139, J169, and J179 IP Phones used with Avaya Aura®, Avaya IP Office™, and select 3PCC (3rd party call control platforms). J100 SIP 4.0.0.0 software will not load or operate on any other models.

This release supersedes all previous Avaya J100 Series SIP software releases. Avaya recommends that all customers using Avaya J100 Series SIP software upgrade to this version at their earliest convenience.

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

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

Copyright Avaya 2018 All rights reserved

Compatibility

The Avaya J129, J139, J169 and J179 IP Phones using J100 SIP 4.0.0 software is supported with:

- Avaya Aura® Platform 7.0.0.0 (Avaya Aura® Communication Manager 7.0.0.0, Avaya Aura® Session Manager 7.0.0.0, Avaya Aura® System Manager 7.0.0.0) and associated service packs
    - ***Refer to the Advisement section for known limitations if not using 7.1.3.3 or above.***
- Avaya Aura® Platform 7.0.1.0 (Avaya Aura® Communication Manager 7.0.1.0, Avaya Aura® Session Manager 7.0.1.0, Avaya Aura® System Manager 7.0.1.0) and associated service packs
    - ***Refer to the Advisement section for known limitations if not using 7.1.3.3 or above.***
- Avaya Aura® Platform 7.1.0.0 (Avaya Aura® Communication Manager 7.1.0.0, Avaya Aura® Session Manager 7.1.0.0, Avaya Aura® System Manager 7.1.0.0, Avaya Aura® Presence Services 7.1.0.0) and associated feature/service packs
    - ***Refer to the Advisement section for known limitations if not using 7.1.3.3 or above.***
- Avaya Aura® Platform 8.0.0.0 (Avaya Aura® Communication Manager 8.0.0.0, Avaya Aura® Session Manager 8.0.0.0, Avaya Aura® System Manager 8.0.0.0, Avaya Aura® Presence Services 8.0.0.0) and associated feature/service packs
    - ***Refer to the Advisement section for known limitations if not using 8.0.1.0 or above.***
- IP Office™ 10.0 SP7 / 10.1 SP3 (J129 only)
- IP Office™ 11.0 or later for J129/J169/J179
- IP Office™ 11.0 SP1 or later for J129/J139/J169/J179
    - IP Office™ 11.0 FP4 or later for support of Bluetooth on J179
- Avaya Aura® Call Center Elite 7.0.1.0[1], 7.1.0.0[1], 8.0.0.0[1]
- 3PCC (3rd party call control) Platform
    - Broadsoft Broadworks R22.0
    - Zang Office R1.0
    - Edgewater Network device (Edgemarc 4550).

Refer to https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml?name=J100+-+SIP&version=4.0 for an up-to-date listing of compatible products.

New Features in J100 SIP 4.0.0

Avaya J100 Series SIP Release 4.0.0 contains the following new features.

[1] J169/J179 IP Phone are supported with CC Elite. The J129/J139 IP Phone are not supported with CC Elite.

Copyright Avaya 2018 All rights reserved

New with this release	Description
Support for Bluetooth® Wireless Headsets	Bluetooth is available on the J179 and requires an additional Wireless/Bluetooth®[2] hardware module. • Bluetooth® Version 4.2 • Supports Handsfree profile and Headset profile. • Up to six headsets can be paired • Bluetooth® power class 2 (10 meter range) • Status icon shows on phone screen top line when Bluetooth® is enabled. Note: *Support for Bluetooth® with IP Office requires IP Office 11.0 FP4 or later software.*
Improved interworking with Broadsoft.	J100 4.0.0.0 has expanded Broadsoft feature capabilities to include: - Feature support through XSI - Shared Call Appearances - Busy Lamp Field - Corporate Directory Access - Silent Alerting, Ring Splash, Distinctive Ring, Intercom Paging, Anonymous Call Block, Auto Callback, Hot Desking - Call Park - Broadworks Anywhere and Mobility - Simultaneous Ring - DND and Call Forwarding - Redundancy and Resiliency
Improved support for IPv6	J100 4.0.0.0 adds support for the following: - Address assignment via SLAAC (based on MAC) - Resolution of domain names into IPv6 addresses (AAAA records) - IPv6 support for HTTP/HTTPS, SNTP, SCEP, SSH/Telnet, SNMP
Support J100 Expansion Module (JEM24)	Support J100 Expansion Module with 24 red/green indicator buttons. Display is color with J179 IP Phone and grayscale with J169 IP Phone. Up to three modules can be attached to the J169/J179.
Support for Avaya L100 Headsets	Avaya L100 headsets are supported.
New backgrounds/screensavers	The J169/J179 include six built-in background images and six built-in screensavers which are coordinated with attached JEM24(s).
Traditional Chinese font support	J139/J169/J179 now support Traditional Chinese fonts. The J129 does not support Traditional Chinese fonts.

[2] The Bluetooth® word mark and logos are registered trademarks owned by the Bluetooth SIG, Inc. and any use of such marks by Avaya is under license.

Copyright Avaya 2018 All rights reserved

New with this release	Description
Improved web interface	The web administration interface has been enhanced to include: - “help” information on parameters - identification of source of configured parameter on phone - ability to modify some parameters without invoking a reboot of the IP Phone
SCEP with AES256	SCEP has been enhanced to support AES256 encryption

Copyright Avaya 2018 All rights reserved

Documentation for J100 SIP 4.0.0.0

The following documentation has been updated for this release:

- J100 Series IP Phone Overview and Specifications
- Installing and Administering Avaya J100 IP Phones
- Using Avaya J129 IP Phone SIP
- Using Avaya J139 IP Phone SIP
- Using Avaya J169/J179 IP Phone SIP
- Using JBM24 Button Module
- Using Avaya J100 Expansion Module
- Avaya J129 IP Phone Quick Reference
- Avaya J139 IP Phone Quick Reference
- Avaya J169/J179 IP Phone Quick Reference
- Using Avaya J100 series IP phone for Call Center Agents
- Avaya J129 IP Phone in third party call control setup Quick Reference guide
- Avaya J139 IP Phone in third party call control setup Quick Reference guide
- Avaya J169/J179 IP Phone in third party call control Quick Reference Guide
- Using Avaya J129 IP Phone SIP in third party call control setup
- Using Avaya J139 IP Phone SIP in third party call control setup
- Using Avaya J169/J179 IP Phone SIP in third party call control setup
- Installing and Administering Avaya J100 Series IP Phones in third party call control setup

These documents are available on http://support.avaya.com under "J100 Series IP Phones " -> "SIP 4.0.x" -> Documents

Copyright Avaya 2018 All rights reserved

J100 SIP 4.0.0.0 (4.0.0.0.21) Package Content

The J100 SIP 4.0.0.0 package (J100-IPT-SIP-R4_0_0_0-120618.zip) contains all the files necessary to upgrade Avaya new or previously installed Avaya J129/J139J169/J179 IP Phones to the J100 SIP 4.0.0.0 software.

- FW_S_J129_R4_0_0_0_21.bin – application binary file for J129
- FW_S_J139_R4_0_0_0_21.bin – application binary file for J139
- FW_S_J169_R4_0_0_0_21.bin – application binary file for J169
- FW_S_J179_R4_0_0_0_21.bin – application binary file for J179
- FW_JEM24_R1_0_0_0_15.bin – application binary file for the JEM24
- J100Supgrade.txt – This file is downloaded by the IP Phones and instructs the phone on how to upgrade to this version of software
- Predefined language files for phone display:
  - Mlf_J129_BrazilianPortuguese.xml
  - Mlf_J129_CanadianFrench.xml
  - Mlf_J129_CastilianSpanish.xml
  - Mlf_J129_Chinese.xml
  - Mlf_J129_Dutch.xml
  - Mlf_J129_English.xml
  - Mlf_J129_German.xml
  - Mlf_J129_Hebrew.xml
  - Mlf_J129_Italian.xml
  - Mlf_J129_Japanese.xml
  - Mlf_J129_Korean.xml
  - Mlf_J129_LatinAmericanSpanish.xml
  - Mlf_J129_ParisianFrench.xml
  - Mlf_J129_Polish.xml
  - Mlf_J129_Russian.xml
  - Mlf_J129_Turkish.xml
  - Mlf_J139_Arabic.xml
  - Mlf_J139_BrazilianPortuguese.xml
  - Mlf_J139_CanadianFrench.xml
  - Mlf_J139_CastilianSpanish.xml
  - Mlf_J139_Chinese.xml
  - Mlf_J139_Dutch.xml
  - Mlf_J139_English.xml
  - Mlf_J139_German.xml
  - Mlf_J139_Hebrew.xml
  - Mlf_J139_Italian.xml
  - Mlf_J139_Japanese.xml
  - Mlf_J139_Korean.xml
  - Mlf_J139_LatinAmericanSpanish.xml
  - Mlf_J139_ParisianFrench.xml
  - Mlf_J139_Polish.xml
  - Mlf_J139_Russian.xml
  - Mlf_J139_Thai.xml
  - Mlf_J139_Traditional_Chinese.xml
  - Mlf_J139_Turkish.xml
  - Mlf_J169_J179_Arabic.xml
  - Mlf_J169_J179_BrazilianPortuguese.xml

Copyright Avaya 2018 All rights reserved

  - Mlf_J169_J179_CanadianFrench.xml
  - Mlf_J169_J179_CastilianSpanish.xml
  - Mlf_J169_J179_Chinese.xml
  - Mlf_J169_J179_Dutch.xml
  - Mlf_J169_J179_English.xml
  - Mlf_J169_J179_German.xml
  - Mlf_J169_J179_Hebrew.xml
  - Mlf_J169_J179_Italian.xml
  - Mlf_J169_J179_Japanese.xml
  - Mlf_J169_J179_Korean.xml
  - Mlf_J169_J179_LatinAmericanSpanish.xml
  - Mlf_J169_J179_ParisianFrench.xml
  - Mlf_J169_J179_Polish.xml
  - Mlf_J169_J179_Russian.xml
  - Mlf_J169_J179_Thai.xml
  - Mlf_J169_J179_Traditional_Chinese.xml
  - Mlf_J169_J179_Turkish.xml
- Eight extended Korean ring tone files:
  - KoreanRT1.xml
  - KoreanRT2.xml
  - KoreanRT3.xml
  - KoreanRT4.xml
  - KoreanRT5.xml
  - KoreanRT6.xml
  - KoreanRT7.xml
  - KoreanRT8.xml
- One certificate file:
  - av_prca_pem_2033.txt – Avaya Product Root CA certificate with an expiration date of 2033
- Avaya-J100IpPhone-MIB.mib – mib file
- release.xml
- A “signatures” subdirectory containing signature files and a certificate file. Both SHA-1 and SHA-256 signature files are included
- Avaya Global Software License Terms 102016v1.pdf

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

Copyright Avaya 2018 All rights reserved

Advisements with J100 SIP 4.0.0.0 software

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

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

3PCC Hardware – cannot be used with Avaya Aura® or Avaya IP Office™

Customers can purchase "3PCC" versions of the J129/J139/J169/J179 hardware which are pre-configued for interworking with Open SIP platforms such as Broadsoft and Zang Office. **When using J100 3.0.0.1 or later software, the "3PCC" hardware cannot be converted for use on Avaya Aura® or Avaya IP Office™.**

J179 with Expansion Modules (JBM, JEM24) modules – 5 volt power supply may be required

- There are certain power requirements when connecting either the JBM or JEM24 expansion modules to the phone. Depending upon the amount of power supplied by the power source over Ethernet, it may be necessary to power the phone by a separate 5 Volt power supply. Please see the *Power Specifications* section in the Installing and Administering Avaya J100 IP Phones

J129/J139/J169/J179 – Aura Feature Provisioning Limitations

Avaya Aura® Communication Manager 7.1 and below does not provide native support of the J129/J139/J169/J179 IP Phones. The J129 should be administered as a "9608SIP", the J139 as a "9608SIP", the J169 as a "9611SIP" or "9611SIPCC" and the J179 as a "9611SIP" or "9611SIPCC".

Avaya Aura® 8.0.1 provides native support of the J129/J169/J179 IP Phones. The J139 should be administered as J169.

When using Avaya Aura® 7.1 (and below) and J100 4.0.0.0 (and below) there are feature administration limitations. With this configuration anything configuration provided by SMGR will be applied to the user at first login. Changes to SMGR after first login will not be applied to the J100 "Phone Screen". **See the table below for further details.**

Service Packs to allow for administration of J100-Series IP Phones on Avaya Aura 7.1.3.3 have been provided by Avaya. Avaya strongly recommends that all customers using J100-series IP Phones upgrade to these service packs. There are two software components to deliver this solution:

1. A System Manager 7.1.3.3 Service Pack identified via PCN2062Su.

2. A Session Manager 7.1.3.3 Service Pack identified via PCN2068Su.

Session Manager PSN PSN005267u details the main operational changes and a list of things that should be considered when rolling out this solution, including some differences that may be seen when both J100-Series IP Phones and 9600-Series IP Phone are used within the same environment.

Copyright Avaya 2018 All rights reserved

Note: Be sure to read the PSN before rolling out the software changes to the servers.

	Phone operations (User logs in for the very first time)	**Phone operations (SMGR Add, Move Features and Autodials after user has logged in)**	**Phone operations (User changing label)**	**Phone operations (User moving/adding a feature / auto dial to a different line location on the phone)**	**Phone operations (User delete a feature / auto dial using customization)**	**Phone operations (Customization -> Restore)**
Admin using Aura pre Aura 7.1.3.3: - J100 phone configured as 9600 on SMGR.	All features and auto dials will show on the phone and button module at the line locations as defined in SMGR. Labels defined in SMGR will not show. **Phone will show default labels.**	New Favorite features/pre-configured autodials will NOT show up on Phone screen. Moved Favorite feature/auto-dial will not show up in the phone screen and will cause the original key to disappear. [3]	Label change will not show in SMGR.	Change will not show in SMGR (similar behavior as SIP 9600-series IP deskphone)	No change in SMGR.	All features and autodials will show on the phone and button module at the line locations defined in SMGR. Phone will show default labels. No change in SMGR.
Admin using Aura 7.1.3.3: - J100 phone configured as 9600	All features and auto dials will show on the phone and button module at the line locations as defined in SMGR. Labels defined in SMGR will show.	New Favorite features/pre-configured autodials will NOT show up on Phone screen. Moved Favorite feature/auto-dial will not show up in the phone screen and will cause the original key to disappear. [3]	Label change will show in SMGR.	Change will not show in SMGR (similar behavior as SIP 9600-series IP deskphone)	No change in SMGR.	All features and autodials will show on the phone and button module at the line locations defined in SMGR. Phone will show default labels. No change in SMGR.
Admin using Aura 8.0.1 - J100 phone configured as J100	Features and auto dials marked as favorites will show on the phone and button locations. Features not marked as favorites will only show in the Feature menu. Pre-configured Autodials not marked as Favorites will show up only during end user customization. The phone will show the labels defined on keys marked as Favorites in SMGR on the Phone screen.	New Favorite features/pre-configured autodials will show up on Phone screen. Moved Favorite feature/auto-dial will show up in the phone screen.	Label change will show in SMGR.	Change will not show in SMGR (similar behavior as SIP 9600-series IP deskphone)	Feature favorite flag will be unchecked in SMGR	All features and autodials marked as favorites will show on the phone and button module at the line locations. No change in SMGR. Phone will show labels as defined in SMGR.

[3] J100 4.0.0.1 Service Pack and feature enabled, J100 will auto populate Features/Autodials if less than Aura 8.0.1 and added/moved keys will not disappear.

Copyright Avaya 2018 All rights reserved

Using Bluetooth headsets on Broadsoft - limitations

In certain scenarios (listed below) it will not be possible to get an "incoming call notification" in the Bluetooth headset (usually a short beep) nor will it be possible to answer a call using the button on the Bluetooth headset. However, it will be possible to see the incoming call on the phone screen and to hear the ringing on the phone AND it will be possible to answer the call using either the Answer Softkey on the phone or the Headset button on the phone.

The following features have this limitation.

- Busy Lamp Field (BLF) – An incoming BLF alerting notification
- Call Park – A call retrieve alerting notification
- Shared Call Appearance (SCA) – An incoming SCA notification

Limitations with IPv6

J100 1.5.0 and later includes support for IPv6 interworking. The following are known limitations of the J100 4.0.0 or later implementation:

- Broadsoft Interoperability
- Extended rebind
- LLDP configuration of IPv6 related settings is not supported
- Microsoft Exchange integration over IPv6 must use an FQDN for EXCHANGE_SERVER_LIST. i.e. SET EXCHANGE_SERVER_LIST exch1.myco.com
- The following functionality is only supported via IPv4
    - RTCP
    - Push
    - Avaya Diagnostic Server (ADS / SLAMon)
    - Shared Control / Deskphone Mode
    - Interworking with CC Elite.

SSH – Remote Access (EASG)

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

Support for SHA2-signed software files

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

Removal of Avaya SIP Root CA Certificate

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

Copyright Avaya 2019 All rights reserved

Support for OCSP

J100 SIP software supports OCSP (Online Certficate Status Protocol) for checking whether certificates presented to the phone by servers are good, revoked, or unknown. If a certificate is revoked, the TLS connection will not be established or will be closed (in the case of an ongoing TLS connection). OCSP is supported for 802.1x (EAP-TLS), SIP over TLS, and HTTPS.

MLPP – Limitations during a server failure

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

Bi-Directional EHS – Compatible Headsets

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

J169 IP Phone – Minimum Software Release

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

J179 IP Phone – Minimum Software Release

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

Microsoft Exchange Integration using EWS

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

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

Debug mode

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

Copyright Avaya 2019 All rights reserved

SIP_CONTROLLER_LIST

This parameter consolidates SIP controller parameters for IP address, port, and transport protocol into a single configuration parameter. The parameter setting should be a list of controller information where the format for each controller entry is "host:port;transport=xxx" . The host should be specified only by an IP address when interworking with Avaya Aura™. The use of Fully Qualified Doman Names (FQDN) is only supported in IP Office and 3PCC environments. This applies to all sources of the SIP_CONTROLLER_LIST parameter which includes DHCP, LLDP, Web interface and the 46xxsettings.txt file

Security Certificates – IP Address versus FQDN

There is an industry movement towards the use of a FQDN (Fully Qualified Domain Name) instead of an IP address for the Subject Alternate Name or Subject Common Name for security certificates. J100 software supports a FQDN_IP_MAP parameter which specifies mapping of FQDNs to IP addresses for the purpose of validating an FQDN identity found in a server certificate.

SRTP (Media Encryption)

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

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

J100 software supports AES-256 media encryption. Care must be taken to properly configure the encryption parameter when this is used in conjunction with other devices that do not support AES-256.

EAP TLS

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

Multi Device Access

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

Copyright Avaya 2019 All rights reserved

Language support

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

Ringtone and Ringtone Wave Files

Numeric only naming conventions should be avoided with ringtone names (E.g. 12345.wav). The maximum allowed size of an individual ringtone file is 512 KB. The maximum allowed size of all ringtone files is 5120 KB.

Headset Profiles

J100 SIP 1.5.0.0 and later software supports "Headset Profiles"[4] to provide optimum performance for different brands of headsets. An up-to-date version of the profile <-> vendor cross reference can be found at https://downloads.avaya.com/css/P8/documents/100173755.

Avaya Session Border Controller for Enterprise

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

SET WAIT_FOR_REGISTRATION_TIMER 40

SIP Transport Protocols

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

Encryption – SHA2 and RSA 2048

J100 software supports RSA 2048 bit length encryption keys and supports the SHA2 (224, 256, 384, and 512) hash algorithm. This has been certified for HTTPS usage for web-based administration of these phone sets. When the TLS server-client handshake is initiated, this IP Phone (operating as the client) is able to send its Identity certificate with an enhanced digital signature (SHA2/2048 key). Additionally, this IP Phone is able to receive and validate server Identity certificates which have an enhanced digital signature (SHA2/2048 key).

Interworking – Avaya Diagnostic Server (ADS)

Avaya J100 SIP Release 2.0.0.0 and later supports the ADS server. The SLMSRVR parameter must be set in the 46xxsettings.txt file for this version of the agent to register with ADS. In addition, a valid certificate file must be downloaded via TRUSTCERTS.

Avaya Diagnostic Server 3.0.3 is the minimum release to support the J129 IPhone, the J169 IP Phone and the J179 IP Phone.

Avaya Diagnostic Server 3.0.4 is the minimum release to support the J139 IP Phone.

[4] J129 does not support a headset

Copyright Avaya 2019 All rights reserved

"Desk Phone" Mode and Lock

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

Demo Certificates – Avaya Aura® Session Manager 6.3.8 and newer

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

Interworking – TLS 1.2

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

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

J129/J139 - Presence

The J129 does not display presence in an Avaya Aura® network or have the ability to manually set a presence state. The J129 publishes presence information for other clients that support viewing presence.
The J139 displays presence and publishes presence but does not have the ability to manually set a presence state.
The J169 and J179 both display presence, publish presence, and have the ability to manually set a presence state

Copyright Avaya 2019 All rights reserved

VLAN separation

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

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

Features not supported on the J129 Phone

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

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

Features not supported on the J139 Phone

The following features are not supported by the J139 IP Phone with J100 software:

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

J139 with IP Office – Features supported / not supported

The following features are supported by the Avaya J139 IP Phone when deployed on IP Office™:

- Basic call handling on *Call Appearances and Line Appearances only* – Making a call, Call presentation, Answer, Hold, Transfer, Conference, Drop
- IP Office Directory (Personal and System)
- IP Office Call History
- Visual Voice

Include basic operation and call handling feature controls by default via IP Office Features Menu

- DND
- Forwarding

Copyright Avaya 2019 All rights reserved

- Mobile Phone Call Twinning (User must first be administered to permit Mobile Twinning by a system Administrator).
- Hot Desking

Allow basic call handling feature controls to be administered as button features by a system Administrator

- Call Park
- Call Pickup
- Call Page
- Call Recording
- Auto Call-back
- Account Code
- Authorisation Code

Allow basic agent controls to be administered as button features by a system Administrator

- Hunt Group Membership
- Agent Status
- After Call Work
- Coaching Request

The following features are <u>not</u> supported by the Avaya J139 IP Phone when deployed on IP Office™:

Advanced Call Presentation / Handling:

- MADN
- Bridged Appearances
- Coverage Appearances
- User BLF
- Group BLF

IP Office Features/Status Menus:

- Advanced Call Pickup
- Advanced Call Park
- DND exceptions
- Account / Authorisation Code
- Auto Answer Controls
- Withhold Number
- Coverage Ring Controls
- Advanced Hunt Group Controls: (Multi Membership, Group Status, Group Configuration)
- Self-Administration
- System Administration

Button configuration:

- Hands-free Answer
- Automatic Intercom
- Specific Call Dial Types
- Conference Meet-Me
- Self-Administration
- System Administration

Copyright Avaya 2019 All rights reserved

- Advanced Hunt Group Controls (Group Status, Group Configuration)
- Agent Supervisor Features: (Call Steal, Call Listen, Call Intrude, Coaching Intrusion)

J169/J179 with IP Office – Features supported / not supported

The following features are supported by the Avaya J139 IP Phone when deployed on IP Office™:

- Basic call handling on *Call Appearances and Line Appearances only* – Making a call, Call presentation, Answer, Hold, Transfer, Conference, Drop
- IP Office Directory (Personal and System)
- IP Office Call History
- Visual Voice

Include basic operation and call handling feature controls by default via IP Office Features Menu

- DND
- Forwarding
- Mobile Phone Call Twinning (User must first be administered to permit Mobile Twinning by a system Administrator).
- Hot Desking

Allow basic call handling feature controls to be administered as button features by a system Administrator

- Call Park
- Call Pickup
- Call Page
- Call Recording
- Auto Call-back
- Account Code
- Authorisation Code

Allow basic agent controls to be administered as button features by a system Administrator

- Hunt Group Membership
- Agent Status
- After Call Work
- Coaching Request

The following features are also supported by the Avaya J169/J179 IP Phone when deployed on IP Office™:

Advanced Call Presentation / Handling:

- MADN
- Bridged Appearances
- Coverage Appearances
- User BLF
- Group BLF

Copyright Avaya 2019 All rights reserved

IP Office Features/Status Menus:

- Advanced Call Pickup
- Advanced Call Park
- DND exceptions
- Account / Authorisation Code
- Auto Answer Controls
- Withhold Number
- Coverage Ring Controls
- Advanced Hunt Group Controls: (Multi Membership, Group Status, Group Configuration)
- Self-Administration
- System Administration

Button configuration:

- Hands-free Answer
- Automatic Intercom
- Specific Call Dial Types
- Conference Meet-Me
- Self-Administration
- System Administration
- Advanced Hunt Group Controls (Group Status, Group Configuration)
- Agent Supervisor Features: (Call Steal, Call Listen, Call Intrude, Coaching Intrusion)

The following features are not supported by the Avaya J169/J179 IP Phone when deployed on IP Office™:

- Personalization (i.e. ability to reconfigure the button layout)
- Push API

Deploying the J129/J139/J169/J179 in 3PCC Platform

The J129/J139J169/J179 are supported with Broadsoft Broadworks R21SP1, Zang Office R1.0. IP phone configuration file (settings file) must be deployed from a file server (HTTP or HTTPS). User backup/restore must also be deployed from a file server (HTTP or HTTPS). SIP Transport = TLS is not supported. For these phones to work in 3PCC environment, configuration file (settings file) must have following parameter configured with value as given:

– SET ENABLE_AVAYA_ENVIRONMENT 0
– SET DISCOVER_AVAYA_ENVIRONMENT 0
– SET ENABLE_IPOFFICE 0

- See Installing and Administering Avaya J100 Series IP Phones in third party call control setup for more detail.

Copyright Avaya 2019 All rights reserved

Provisioning of File Server Address

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

- DHCP
- LLDP
- Device Interface
- Device Enrolment Service (DES)

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

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

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

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

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

Note:

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

Copyright Avaya 2019 All rights reserved

J100 4.0.0.0 Resolved Issues (since J100 3.0.0.2)

The following table includes issues which are resolved with this release of software compared to J100 3.0.0.2.2

External ID	Internal ID	Issue Description
Avaya Aura®		
	SIP96X1-34721	Phone displays incorrectly after recording audio.
	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.
	SIP96X1-29926	J129- One way speech path after holding/resuming the call with codec OPUS-WB20k and media encrytion 3-srtp-aescm128-hmac80-unauth.
	SVCI-4023	SLA server cannot start Agent Remote Control on J100 phone
IP Office		
	SIP96X1-31066	J179 - Headset call - make hold/unhold call goes to handsfree on speaker
3PCC		
	SIP96X1-32258	Phone has no configuration (i.e. direct from factory or after a "Clear" operation) and the web interface is used to configure the SIP controller list and user information. The phone does not login when rebooted.
All Platforms		
	SIP96X1-23890	J129 - "@" character is not supported for User ID, Contacts. If "@" character is configured, phone will ignore all the characters after "@" including "@" character. For CLI display, phone will not display name or number after "@" including "@" character.
Web User Interface		
	SIP96X1-34440	If a phone is on an active call and the Web UI is used at the same time to upgrade software, then voice path is lost.
	SIP96X1-34441	Phones do not reboot automatically after upgrading software via Web UI.
	SIP96X1-30908	Web UI - Need to clarify item Old Web Admin Password in Phone Admin Password menu
	SIP96X1-34875	Quality of Service page incorrectly shows Ethernet QoS when running in WiFi mode.
	SIP96X1-32880	Web UI – If ony the ENABLE_3PCC_ENVIRONMENT value is changed, then it does not take affect.

Copyright Avaya 2019 All rights reserved

External ID	Internal ID	Issue Description
	SIP96X1-30510	Web UI displays SIP User ID and Authentication User ID inconsistently after Guest User is logged out.

Copyright Avaya 2019 All rights reserved

Unresolved issues in J100 4.0.0.0

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

External ID	Internal ID	Issue Description
	Avaya Aura®	
1-12671341066	SIP96X1-24119	ELD Rules not working. User is not able to dial 11 digit national calls from history.
	SIP96X1-20240	Phone B is configured with EC500 feature with cell phone number. Make call from phone A to phone B and answer the call on Cell phone. Press bridge soft key on phone B, then from phone B make unattended transfer to phone C. Answer the call on C -> No voice speech path between phone A and C.
	SIP96X1-23977	Deskphone is configured for FIPS mode and has a valid identity certificate. If an attempt is made to install a new certificate which is not FIPS-compliant, then the Deskphone does not display a “certificate rejected” message but does continue to use the original valid certificate.
	SIP96X1-23938	J129 Phone doesn't display "Non-AST/Fail-Over" icon after failover to non-AST environment when you are not on the idle screen and failover happens.
	SIP96X1-23905	J129 phone does not play ringing tone for second call when active call is emergency call
	SIP96X1-23883	J129 – Phone does not generate call log of Emergency call in Locked state when Emergency number was added in Contacts
	SIP96X1-23863	J129 – Phone does not always update sip proxies list after changing order of sip proxies in SMGR
	SIP96X1-23238	J129 - Phone displays conference icon and softkeys after other MDA user deactivates call-park feature
	SIP96X1-20779	J129 - Phone does not enable call-park feature when the feature is activated from another MDA user
	SIP96X1-20316	J129 - Server field ID display does not index to the right after clearing 8 characters
	SIP96X1-26755	J129 - Local call forward does not appear on Feature screen for using after failover to Audiocodes
	SIP96X1-28106	Phone does not display NewCall SK for making the second calls after completing failover to BSM in active call
	SIP96X1-28113	Guest Login: History LED keeps on lit, on primary user even after guest login logs out

Copyright Avaya 2019 All rights reserved

External ID	Internal ID	Issue Description
	SIP96X1-28284	Navigation does not work for the first pressing in “EAP-MD5 Authentication failed” screen
	SIP96X1-28651	Unexpected Softkeys after Cancel consult with 3rd party
	SIP96X1-29823	J179 phone does not display added contact during limbo state
	SIP96X1-29855	Intermittent - Phone is stuck at PKCS12 installation screen during boot up in Wifi mode
	SIP96X1-30262	Remote Control icon is not getting displayed for logged out J169 phones
	SIP96X1-31097	Parameter PKCS12_PASSWD_RETRY works incorrectly.
	SIP96X1-31177	J100 phones take time to perform ‘hold/transfer’ SK operation if these SKs are pressed after recording an active call.
	SIP96X1-31276	Phone displays “No match found” when searching contact which created with only Last name on Exchange Server
	SIP96X1-31692	J139 – Call Forward Ringtone does not work.
	SIP96X1-36019	The pop-up entry doesn’t disappear after using “Dial Intercom” to dial
	SIP96X1-44264	After reset to defaults, dual phone displays ‘Acquiring service’ icon although phone can login extension successfully *Work-around:reboot phone*
1-14541450549	SIP96X1-49140	Favorite and Label for a new feature added to J179 using SMGR 8.0.1 are removed by the phone
IP Office		
	SIP96X1-23804	J129 contacts with IP Office: Sometimes ‘New’ softkey is displayed after adding 250 contacts.
	SIP96X1-35056	J169/J179 phones require additional reboot to function normally in IPO-CCMS environment if they get incorrect SIP proxy IP in previous reboot.
	SIP96X1-33444	"Reset to defaults" fails on J179 while registered to Branch IPO
	SIP96X1-36922	J129 – IPO - Phone A displays "Acquiring service" and Phone B cannot login to phone A when phone B tries to log into phone A's extension
1-13926266159	SIP96X1-31884	139 169 J179 - Handset rapid on/off hook selects handsfree transducer *Workaround: Set System>Telephony>Tones & Music>Disconnect Tone settings on the IP Office to Off.*
CCElite		
	SIP96X1-31004	Phone does not display full AgentID when system language set to English and phone set to Arabic
	SIP96X1-40958	Phone does not display UU-info when moving line CA from phone screen to button module.
	SIP96X1-36054	J169/179 – CCElite - LED state of Auto-in/Manual-in feature button flutters instead of flash

Copyright Avaya 2019 All rights reserved

External ID	Internal ID	Issue Description
	SIP96X1-44374	[CCElite] Backlight doesn't turn on when Agent receives DAC call in aux work mode
1-14546691793	SIP96X1-49615	J169 Agent logout button is not working from main screen if the agent logout reason code is required or optional. *Workaround: use logout feature from Feature screen or set reason code to "none"*
1-14553411646	SIP96X1-49685	J169 in CC assist button keeps flashing after the call to supervisor is dropped
1-14560990960	SIP96X1-49188	J179 SIP CC do not go to Aux mode
3PCC		
	SIP96X1-23559	J129 - User_Store - Phone is not making PUT request after receiving 404 in response of a GET query after adding first contact if HTTP Authentication is enabled in server and Authentication is ignored by user when it prompts. *Workaround: Edit contact again and perform Manual Backup*
	SIP96X1-23211	J129 - Glare handling for retransmitted INVITE and 407 with different nonce *Workaround: Change Timer T1*
	SIP96X1-23183	J129 - User_Store - If user changed a parameter that triggered a Backup. If the backup is in progress and the user logs out and new user is logging immediately may have their "restore" impacted and it may not work.
	SIP96X1-42012	L129 BT headset does not hear ringing tone after when ignore one of incoming calls (RTX 209114)
	SIP96X1-43220	[3PCC mode] Unable to login as BroadWorks user with error of "acquiring service" when application server FQDN addre ss is given in SIP_CONTROLLER_LIST2 *Workaround: 3PCC over IPv6 is not supported, use SIP_CONTROLLER_LIST*
	SIP96X1-41164	HTTP redirect to HTTPS fails certificate validation, connection fails *Workaround: reconfigure phone URL to HTTPS*
	SIP96X1-44395	When SCA PRIMARY_LINE_TYPE 1 and AS1 and AS2 offline and back, Stuck Acquiring services *Workaround: reboot phone*
	SIP96X1-44392	[Broadsoft 3PCC] Cannot login user after rebooting when authentication password is changed on portal and not in settings *Workaround: update settings file with new password*
	SIP96X1-44509	Unable to view members of Broadsoft directories when in the Groups view *Workaround:press Contacts, highlight the Broadsoft Directory and press "Members" softkey*

Copyright Avaya 2019 All rights reserved

External ID	Internal ID	Issue Description
All Platforms		
	SIP96X1-22231	J129 - MIB browser displays value of “endptLANGINUSE” incorrectly
	SIP96X1-21314	J129 - Phone does not allow contacts to be added as speed dial entries until PPM update is complete
	SIP96X1-23850	J129 - When downgrade fails, Upgrade info screen is blank
	SIP96X1-23791	J129 - 802.1x – Phone is not displaying 802.1x credential screen if phone receives EAP-Failure packet. This case happens only if credentials are changed in Radius Server during working environment. *Workaround: Reboot the phone*
	SIP96X1-20743	J129 - Phone reboots a second time after the user comments out the proxy address in settings file.
	SIP96X1-20372	J129 - Phone does not display SCEP notifications while it is downloading identity certificate from CA server
	SIP96X1-29607	[DES] Auto Config prompt is not displayed if DES is manually invoked from Admin Menu
	SIP96X1-30718	Phone display message “ Contact already exists” when edit ringtone
	SIP96X1-30715	Phone display "Feature not available" while customizing line keys
	SIP96X1-30948	Phone displays number of BCA incorrectly after moving in customize key.
	SIP96X1-31080	Pressing key "0" for the first input in contact group name then press other key, other key is doubled
	SIP96X1-33023	Unable to gracefully recover phone when lost WIFI on active call
	SIP96X1-34870	When adding a new group in Contact groups, the “NAME” prompt is not translated to some languages.
	SIP96X1-31991	Phone does not process SCEP request with new change for MYCERTCN or MYCERTURL *Workaround: Remove old identity certificate (SET DELETE_MY_CERT 1) then install new cert.*
	SIP96X1-41860	J129 "Redial" softkey disappears on dialing screen after calling to phone which actived feature "CFW all"
	SIP96X1-33445	J100 gets locked in the first time after Phone Lock Idle Time is changed to 0
	SIP96X1-37721	Phone displays restaring forever after clearing phone *Workaround: restart the phone*
	SIP96X1-41905	Change Menu>Administration>IP Configration>Auto Provisioning>Service to Active and reboot fails and connects to incorrect HTTPSRVR

Copyright Avaya 2019 All rights reserved

External ID	Internal ID	Issue Description
	SIP96X1-38760	Phone firmware does not diplay on SLA Server after phone get discovered
	SIP96X1-44461	J100 dual mode - Cannot manually change IPv4 address after switching subnets when DHCPv6 fails *Workaround: disable DHCPv6 client (Use DHCP(v6) off in Admin menu)*
	SIP96X1-44420	Dual mode phone stays at "Starting..." screen when manual IPv4 and no DHCPv6 server in network (setting "Use DHCPv6" is Yes) *Workaround: disable DHCPv6 client (Use DHCP(v6) off in Admin menu)*
	SIP96X1-43649	[Intermittent] Speaker LED may stay on when the call is dropped by far end *Workaround: reboot the phone*
	SIP96X1-48772	[IPv6] the prefixes from "0000:" to "0FFF:" unable to use
Web User Interface		
	SIP96X1-41670	Last extension is hidden when logout user with Arabic language is changed from Web UI.
	SIP96X1-44201	Web displays wrong SIP Proxy Server when phone switch from SIP proxy IPv4 to IPv6 or from SIP proxy IPv6 to IPv4
	SIP96X1-41142	Icon presence does not work after when enable presence on Web UI
	SIP96X1-44261	The Web does not display Sources of SIP proxy list when dual phone gets SIP proxy list by SIP_CONTROLLER_LIST.
	SIP96X1-44209	Phone does not update configuration parameter of SCAs after importing the settings file to the WEB server
	SIP96X1-41068	HTTP port value from phone UI source is not visible and are deleted if value is undone from web UI
	SIP96X1-39592	Values configured from web are displayed in Phone UI source for parameter IPV4 Address
	SIP96X1-44263	Changing admin password from Web UI doesn' t take effect on phone if phone has not logged-in after doing reset to defaults. *Workaround: set admin password from settings file, DHCP, or PhoneUI*
	SIP96X1-42434	Web UI - Phone does not use new SIP user ID which is set on Web for XSI authentication
Wifi		
	SIP96X1-32364	Phone does not automatically connect when switching to WIFI with WEP secured method *Workaround: Reboot phone, phone connects to new WIFI successfully*

Copyright Avaya 2019 All rights reserved

External ID	Internal ID	Issue Description
	SIP96X1-43068	[Intermittent - Wifi - Bluetooth] Voice lost and not clear when using 2.4GHz Wifi and Bluetooth headset (GES 392) *Workaround: Use 5GHz Wifi*
	SIP96X1-42168	[Intermittent] Phone displays message “No Wi-fi Network chosen. Press Networks to choose a network” after selecting “reset to defaults” *Workaround: Go to admin menu, select reset to defaults again*
	Bluetooth	
	SIP96X1-39594	Phone displays Change default audio path to “Speaker” although phone is disabled speaker when unpairing BT device
	SIP96X1-44056	[BT] – If BT is turned off and default BT headset, cant make a second call from handset without replacing handset to cradle
	SIP96X1-43649	[Intermittent] Speaker button keep turning on when the call is dropped *Workaround: restart the phone*
	SIP96X1-44265	J169/J179 – BT CCMS - Jabra STEALTH bluetooth device can not use multifunctional button when "Audio path" is set to "Speaker"
	SIP96X1-44387	[Bluetooth] Phone does not initialize reconnect to some headsets
	SIP96X1-43114	Intermittent - after phone is in idle state for 13 hours it still displays Bluetooth connected icon on the top line when disconnected *Workaround: re-pair the headset*
	Button Module (JEM24 and JBM24)	
	SIP96X1-43092	JEM24: Power cycle required message dissappears unexpectedly
	SIP96X1-44512	JEM24: Module doesn't reboot overnight after upgrade complete. JEM24 1.0 is running on UTC time. *Workaround: Press Apply Now button to restart module immediately to apply update or wait for a module reach 12.30AM UTC time.*
	BUTTONMODULE-426	JEM24 doesn't report upgrade failure in case of invalid fw file
	BUTTONMODULE-411	CCMS - J169 with JEM24 attached - indentation misaligned for programmed features on JEM24
	BUTTONMODULE-393	JEM24 may ignore Reset to defaults message from phone (Background image may be retained)
	BUTTONMODULE-339	JEM24_The JEM24’s top right-sided label incorrectly aligned when the phone is in CCMS mode
	BUTTONMODULE-383	LED on feature line keys are on again when phone is in locked state and left/right paging keys are pressed

Copyright Avaya 2019 All rights reserved

Appendix 1 – Supported Hardware

J100 SIP 4.0.0.0 software is supported on the following models of IP Phones. Models may ship from the factory with a different load of software pre-installed. As such, they should be upgraded to this release on first installation.

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

Comcode	Short Description	Model	Note
700512392	J129 IP PHONE	J129D01A	
700513638	J129 IP PHONE NO PWR SUPP		
700512969	J129 IP PHONE 3PCC W/O PWR SUPP	J129D01A	
700513639	J129 IP PHONE 3PCC W/CERT		
700513634	J169 IP PHONE NO PWR SUPP	J169D01A	Must use J100 1.5 or later software.
700513635	J169 IP PHONE GSA	J169D01A	Must use J100 1.5 or later software.
700513636	J169 IP PHONE 3PCC	J169D01A	Must use J100 2.0 or later software.
700513569	J179 IP PHONE NO PWR SUPP	J179D02A	Must use J100 1.5 or later software.
700513629	J179 IP PHONE GSA	J179D02A	Must use J100 1.5 or later software.
700513630	J179 IP PHONE 3PCC	J179D02A	Must use J100 2.0 or later software.
700513916	J139 IP PHONE	J139D01A	Must use J100 3.0 or later software.
700513917	J139 IP PHONE 3PCC	J139D01A	Must use J100 3.0 or later software.
700513918	J139 IP PHONE GSA	J139D01A	Must use J100 3.0 or later software.

Copyright Avaya 2019 All rights reserved

Appendix 2 – Release History

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

Release	ID	Date	Link to Readme file
1.0.0.0	1.0.0.0.43	Dec 2016	https://support.avaya.com/css/P8/documents/101033485
1.1.0.0	1.0.0.0.15	Mar 2017	https://support.avaya.com/css/P8/documents/101037079
1.1.0.1	1.0.0.1.3	Aug 2017	https://support.avaya.com/css/P8/documents/101042514
1.5.0.0	1.5.0.0.15	Mar 2018	http://support.avaya.com/css/P8/documents/101047039
2.0.0.0	2.0.0.0.45	April 2018	https://support.avaya.com/css/P8/documents/101048016
3.0.0.0	3.0.0.0.20	July 2018	https://support.avaya.com/css/P8/documents/101050223
3.0.0.1	3.0.0.1.6	Aug 2018	https://support.avaya.com/css/P8/documents/101051793
3.0.0.2	3.0.0.2.2	Nov 2018	https://support.avaya.com/css/P8/documents/101053115
4.0.0.0	4.0.0.0.21	Dec 2018	https://support.avaya.com/css/P8/documents/101054005

Copyright Avaya 2019 All rights reserved

Appendix 3 – New and changed 46xxsettings.txt parameters

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

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

New parameters.

###################### DHCP SETTINGS ######################
DHCPSTDV6 specifies whether DHCPv6 will comply with the IETF RFC 3155 standard and immediately stop using
an IPv6 address if the address valid lifetime 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
a NS (Neighbor Solicitation) request to check for address conflicts, until a REPLY response is received from
a DHCPv6 server (either a new address, or zero lifetimes, or error status codes) or until a DAD conflict is detected.
If the address is duplicated, DHCPv6 client transitions into STOPPED state and the phone reboots.
Value Operation
0 Enter proprietary extended rebinding state (continue to use IPv6 address , if DHCPv6 lease expires) (default)
1 Comply with DHCPv6 standard (immediately release IPv6 address, if DHCPv6 lease expires)
This parameter is supported by:
J100 SIP R4.0.0.0 and later
SET DHCPSTDV6 1

########## NETWORK MODE OF OPERATION ##########
WLAN_MAX_AUTH_FAIL_RETRIES specifies how many times the phone will retry a secure connection upon receiving (possibly successive) auth failures.
Value range is 0-4. The default is 3.
This parameter is supported by:
J100 SIP R4.0.0.0 and later
SET WLAN_MAX_AUTH_FAIL_RETRIES 2
##

################## TRUSTED CERTIFICATES AND GENERAL CERTIFICATES SETTINGS ##################
BLOCK_CERTIFICATE_WILDCARDS specifies whether the endpoint will accept server identity certificates with wildcards.
Value Operation
0 Accept wildcards in certificate (default)
1 Do not accept wildcards in certificates
This parameter is supported by:
J100 SIP R4.0.0.0 and later
SET BLOCK_CERTIFICATE_WILDCARDS 1
##

################ HTTP PROXY SERVER SETTINGS ##############
HTTP_PROXY_CSDK_ENABLE specifies whether CSDK shall use the OS reverse proxy settings if exist.
Value Operation
0 No use of any HTTP proxy by CSDK
1 Enable CSDK to use the HTTP proxy configured in OS, and enforce the HTTP Tunneling in GME without going through the STUN check
if HTTPUA for the call is going through a HTTP proxy.
2 Enable CSDK to use the HTTP proxy configured in OS, and still enable the GME for STUN check before HTTP Tunneling (Default)
This parameter is supported by:
Avaya Equinox 3.4 and later
SET HTTP_PROXY_CSDK_ENABLE 0
##

###################### SCEP SETTINGS #####################
SCEPENCALG specifies SCEP Encryption Algorithm.
Value Operation
0 DES (default)
1 AES-256
This parameter is supported by:
J129 SIP R4.0.0.0 and later

Copyright Avaya 2019 All rights reserved

SET SCEPENCALG 1
##

##
IPv6 related settings are applicable for 96x1 H.323 R6.0 and later, J169/J179 H.323 R6.7 and later, 96x1 SIP R7.1.0.0 and later, J169/J179 SIP R1.5.0 and J100 SIP R2.0.0.0 and later.
PRIVACY_SLAAC_MODE
Valid Values:
0 - Privacy extension disabled, one stable address is generated using modified EUI-64 format interface identifier (Based on MAC address).
The phone address selection preference is based on default RFC6724 SASA rules.
1 - Privacy extension enabled, one stable address is generated using modified EUI-64 format interface identifier (Based on MAC address)
and one temporary private address is generated. The phone address selection preference is based on RFC6724 SASA rules.
PRIVACY_SLAAC_MODE changes default SASA rules (i.e. Rule 7) to prefer a manual, DHCPv6 or Stable SLAAC over SLAAC temporary address. (default)
2 - Privacy extension enabled, one stable address is generated using modified EUI-64 format interface identifier (Based on MAC address) and
one temporary private IPv6 address is generated. The phone address selection preference is based on default RFC6724 SASA rules. Default
SASA Rule 7 is used to prefer SLAAC temporary address over a manual, DHCPv6 or Stable SLAAC addresses.
Definition: Specifies the preference for Privacy Extensions(RFC3041)
This parameter is supported by:
J100 SIP R4.0.0.0 and later
Example:
SET PRIVACY_SLAAC_MODE 2
##
DUAL_IPPREF
Valid Values
4 IPv4 preference (default)
6 IPv6 preference
Description:
DUAL_IPPREF controls:
1. The selection of SSON either from DHCPv4 or DHCPv6 server, when phone is in dual mode, and
2. Whether an IPv4 or IPv6 addresses returned by DNS would be tried first during dual-mode operation.
DHCP clients use DUAL_IPPREF to decide which SSON configuration attributes to apply for DHCPv4/DHCPv6 interworking in dual mode. Based on DUAL_IPPREF the phone selects SSON attributes either from DHCPv4 or DHCPv6 server.
If DNS server name is provided, and if DNS resolver returns both IPv4 and IPv6 addresses, the order in which they will be tried will be based on DUAL_IPPREF parameter.
NOTE: SIP server FQDNs are resolved into addresses that are ordered based on SIGNALING_ADDR_MODE, not DUAL_IPPREF
Example: Setting preference to IPv4
SET DUAL_IPPREF 6
This parameter is supported by:
J100 SIP R4.0.0.0 and later
##

#################### IP OFFICE SETTINGS ####################
ENABLE_OOD_RESET_NOTIFY specifies whether the phone supports out of dialog (OOD) SIP NOTIFY message with
Event:resync or Event:check-sync only. The events are used to remotely restart the phone (once all calls end).
The parameter is used with 3PCC environment only.
Value Operation
0 OOD is not supported (Default)
1 OOD is supported
This parameter is supported by:
J129 J100 SIP R2.0.0.0 and later, J139 SIP R3.0.0.0 and later
SET ENABLE_OOD_RESET_NOTIFY 1
##

################### 3PCC ENVIRONMENT SETTINGS ####################
##
ENABLE_3PCC_ENVIRONMENT specifies whether the deployment environment is third party SIP Server
Value Operation
0 Not 3PCC environment
1 3PCC environment (Default)
Note: This parameter should be set to '0' for Aura environment and IP Office
This parameter is supported by:
J129 SIP R1.1.0.0, J100 SIP R2.0.0.0 and later, J139 SIP R3.0.0.0 and later

Copyright Avaya 2019 All rights reserved

SET ENABLE_3PCC_ENVIRONMENT 0
##
3PCC_SERVER_MODE specifies if the phone expects a generic 3PCC server or a BroadSoft server (applicable when ENABLE_3PCC_ENVIRONMENT is set to 1).
Value Operation
0 Generic (Default)
1 BroadSoft
This parameter is supported by:
J100 SIP R4.0.0.0 and later
SET 3PCC_SERVER_MODE 1
##

######################## BROADSOFT CALL FEATURES SETTINGS ##################
##
The parameters below are applicable when 3PCC_SERVER_MODE=1 and ENABLE_3PCC_ENVIRONMENT=1.
##
BLF_LIST_URI specifies the BroadSoft Busy Lamp Field (BLF) Resource URI. It defines the unique name for the list of users to be monitored.
BLF_LIST_URI must be configured to enable BLF feature unless Xtended Services Interface (XSI) is enabled. When XSI_URL parameter is defined, the phone retrieves BLF configuration from XSP server and
ignores BLF_LIST_URI value. The default value is "".
This parameter is supported by:
J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
SET BLF_LIST_URI sip:mylist1@as.iop1.broadworks.net
SET BLF_LIST_URI mylist1@as.iop1.broadworks.net
SET BLF_LIST_URI sip:mylist1
SET BLF_LIST_URI mylist1
##
CALL_PICKUP_FAC specifies the Directed Call Pickup feature access code that phone will use to pick up the call for a BroadSoft Busy Lamp Field (BLF) monitored station.
The parameter should be provided in BroadSoft environment unless Xtended Services Interface (XSI) is enabled. When XSI_URL parameter is defined, the phone retrieves BLF configuration from
BroadWorks Xtended Service Platform (XSP) server and ignores CALL_PICKUP_FAC value. The default is "*97".
This parameter is supported by:
J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
SET CALL_PICKUP_FAC *98
##
CALL_PICKUP_BARGEIN_FAC specifies the Directed Call Pickup with Barge-in feature access code that phone will use to barge into a call between a remote user
and BroadSoft Busy Lamp Field (BLF) monitored station. This parameter should be provided in BroadSoft environment unless Xtended Services Interface (XSI) is enabled. When XSI_URL parameter is defined,
the phone retrieves BLF configuration from BroadWorks Xtended Service Platform (XSP) server and ignores CALL_PICKUP_BARGEIN_FAC value. The default value is "*33".
This parameter is supported by:
J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
SET CALL_PICKUP_BARGEIN_FAC *32
##
CALL_UNPARK_FAC specifies the Call Retrieve feature access code that phone will use to unpark the call that has been parked for a BroadSoft Busy Lamp Field (BLF) monitored station.
This parameter should be provided in BroadSoft environment unless Xtended Services Interface (XSI) is enabled. When XSI_URL parameter is defined, the phone retrieves
BLF configuration from BroadWorks Xtended Service Platform (XSP) server and ignores CALL_UNPARK_FAC value. The default is "*88".
This parameter is supported by:
J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
SET CALL_UNPARK_FAC *89
##
ALLOW_BLF_LIST_CHANGE specifies the user permissions for adding/removing BroadSoft Busy Lamp Field (BLF) monitored users from the phone.
Value Operation
0 User is not allowed to add/delete BLF monitored users
1 User is allowed only to delete BLF monitored users
2 User is allowed only to add BLF monitored users
3 User is allowed to add and delete BLF monitored users (default)
This parameter is supported by:
J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
SET ALLOW_BLF_LIST_CHANGE 2
##

Copyright Avaya 2019 All rights reserved

##################### BROADSOFT XTENDED SERVICES INTERFACE (XSI) SETTINGS #################
##
The parameters below are applicable when 3PCC_SERVER_MODE=1 and ENABLE_3PCC_ENVIRONMENT=1.
##
XSI_URL specifies BroadWorks Xtended Service Platform (XSP) server FQDN/IP address, HTTP or HTTPS mode and port. If port is not defined, 80 is used for HTTP and 443 for HTTPS by default.
The default is "".
This is the main parameter to make features work in BroadSoft environment.
If value of this parameter is non-empty, phone will initiate Xtended Services Interface (XSI) connections establishment to retrieve feature list.
Note: If XSI_URL is defined the following local call features will not be available. They must be enabled for the user on the BroadSoft server:
- Do Not Disturb (ENABLE_DND, ENABLE_DND_PRIORITY_OVER_CFU_CFB)
- Call Forward CFA, CFB, CFNA
- Auto Answer (ENABLE_AUTO_ANSWER_SUPPORT, AUTO_ANSWER_MUTE_ENABLE)
This parameter is supported by:
J100 SIP R4.0.0.0 and later
SET XSI_URL http://xsp1.iop2.broadworks.net
SET XSI_URL https://xsp1.iop2.broadworks.net:443
SET XSI_URL http://192.168.111.111:8080
SET XSI_URL https://192.168.111.111
##
XSI_CHANNEL_DURATION defines the time duration in minutes for Xtended Services Interface (XSI) event channel, i.e. phone will ask BroadWorks Xtended Service Platform (XSP) server
to maintain the established Comet HTTP connection for the specified period of time. After 50% of this time phone will reestablish Comet HTTP connection.
The values range is 60-1440. The default is 60.
This parameter is supported by:
J100 SIP R4.0.0.0 and later
SET XSI_CHANNEL_DURATION 100
##
XSI_HEARTBEAT defines the interval in seconds to send heartbeat messages over Comet HTTP connection to BroadWorks Xtended Service Platform (XSP) server.
Ideally XSI_HEARTBEAT should be configured to BroadSoft's eventTimeout/2. The eventTimeout value is configurable on
BroadSoft, by default it is 30 seconds.
The values range is 1-999. The default value is 15.
This parameter is supported by:
J100 SIP R4.0.0.0 and later
SET XSI_HEARTBEAT 20
##
FORCE_XSI_USER_ID specifies the BroadSoft's User Id which phone should use for Xtended Services Interface (XSI) authentication (SIP or Web methods).
Note: It shall be User Id without @ and domain. The default is ""
This parameter is supported by:
J100 SIP R4.0.0.0 and later
SET FORCE_XSI_USER_ID userhandle
##
FORCE_XSI_WEB_PASSWORD specifies the BroadSoft's Web portal password which phone should use for Xtended Services Interface (XSI) authentication (Web method).
If empty, it means that SIP authentication method should be used. The default is "".
This parameter is supported by:
J100 SIP R4.0.0.0 and later
SET FORCE_XSI_WEB_PASSWORD userpassword
##

##################### BROADSOFT SHARED CALL APPEARANCE SETTINGS #################
##
The parameters below are applicable when 3PCC_SERVER_MODE=1 and ENABLE_3PCC_ENVIRONMENT=1.
##
PRIMARY_LINE_TYPE specifies if the phones primary line is a private or shared line. The primary line is the one associated with the user's login credentials.
Value Operation
0 Primary line is a private line (default)
1 Primary line is a shared line
This parameter is supported by:
J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
SET PRIMARY_LINE_TYPE 1

Copyright Avaya 2019 All rights reserved

```
##
## PRIMARY_LINE_BARGE_IN_ENABLED specifies whether a primary line which is shared is configured in the BroadSoft server to either enable or disable the ability
## of a user to barge into a call at a different location on the shared line.
## This setting is ignored if PRIMARY_LINE_TYPE = 0
## Value Operation
## 0 Barge in is disabled for the shared line
## 1 Barge in is enabled for the shared line (default)
## This parameter is supported by:
## J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
## SET PRIMARY_LINE_BARGE_IN_ENABLED 0
##
## SCA1_ENABLED, SCA2_ENABLED, SCA3_ENABLED specifies if first, second or third Shared Call Appearance (SCA) is/are enabled.
## For example, SCA1_ENABLED defines if the first shared line is enabled.
## Value Operation
## 0 The shared line is disabled (default)
## 1 The shared line is enabled
## This parameter is supported by:
## J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
## SET SCA1_ENABLED 1
## SET SCA2_ENABLED 1
## SET SCA3_ENABLED 1
##
## SCA1_MAX_CALL_APPEARANCES, SCA2_MAX_CALL_APPEARANCES, SCA3_MAX_CALL_APPEARANCES specify the maximum number of simultaneous calls on the first, second and third shared line
## respectively. Value range 1-5. Default value is 3.
## This parameter is supported by:
## J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
## SET SCA1_MAX_CALL_APPEARANCES 4
## SET SCA2_MAX_CALL_APPEARANCES 5
## SET SCA3_MAX_CALL_APPEARANCES 2
##
## SCA1_SIPUSERID, SCA2_SIPUSERID, SCA3_SIPUSERID specify the AOR(Address of Record) for first, second and third shared line respectively.
## It should only specify the handle (e.g. 123456_2) since the domain is specified independently.
## Note that shared lines are only supported for the same SIP domain as the primary line.
## The default value is "".
## This parameter is supported by:
## J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
## SET SCA1_SIPUSERID 6459137
## SET SCA2_SIPUSERID 6459138
## SET SCA3_SIPUSERID 6459139
##
## SCA1_USERNAME, SCA2_USERNAME, SCA3_USERNAME specify the username to be used for authentication when challenged for credentials on SIP requests associated with
## the first, second and third shared line respectively.
## This value is optional and if not specified the SCA1_SIPUSERID, SCA2_SIPUSERID, SCA3_SIPUSERID would be used for authentication.
## The default value is "".
## This parameter is supported by:
## J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
## SET SCA1_USERNAME 6459137
## SET SCA2_USERNAME 6459138
## SET SCA3_USERNAME 6459139
##
## SCA1_PASSWORD, SCA2_PASSWORD, SCA3_PASSWORD specify the password to be used for authentication when challenged for credentials on SIP requests associated
## with the first, second and third shared line respectively. The default is "".
## This parameter is supported by:
## J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
## SET SCA1_PASSWORD sca1pass
## SET SCA2_PASSWORD sca1pass
## SET SCA3_PASSWORD sca1pass
##
## SCA1_EXTENSION, SCA2_EXTENSION, SCA3_EXTENSION specify the display name for the first, second and third shared line respectively.
## If not specified the SCA1_SIPUSERID, SCA2_SIPUSERID, SCA3_SIPUSERID would be used. The default is "".
## This parameter is supported by:
## J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
```

Copyright Avaya 2019 All rights reserved

```
## SET SCA1_EXTENSION UsernameA
## SET SCA2_EXTENSION UsernameB
## SET SCA3_EXTENSION UsernameC
##
## SCA1_BARGE_IN_ENABLED, SCA2_BARGE_IN_ENABLED, SCA3_BARGE_IN_ENABLED specify for each shared line in the BroadSoft server to either enable or disable the
##  ability of a user to barge into a call at a different location on the first, second, third shared line respectively.
##  Value  Operation
##    0    Barge in is disabled for the shared line
##    1    Barge in is enabled for the shared line (default)
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
## SET SCA1_BARGE_IN_ENABLED 0
## SET SCA2_BARGE_IN_ENABLED 0
## SET SCA3_BARGE_IN_ENABLED 0
##
## SCA_LINE_SEIZE_DURATION specifies the length of time in seconds to be used for a line-seize subscription on any (first, second, third) shared line or on a primary shared line.
##  Value range is 5-40. The default is 15.
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
## SET SCA_LINE_SEIZE_DURATION 0
##
## PROVIDE_SHARED_LINE_CONFIG specifies if the user has the ability to change Shared Line configuration using the Settings menu on the phone.
##  Value  Operation
##    0    Shared lines is not displayed in settings menu
##    1    Shared lines is displayed in settings menu but all information is read-only
##    2    Shared lines is displayed in settings menu and is fully configurable (default)
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (J129 and J139 do not support this parameter)
## SET PROVIDE_SHARED_LINE_CONFIG 0
##

###################### BROADWORKS DIRECTORY SETTINGS #################
##
## The parameters below are applicable when 3PCC_SERVER_MODE=1 and ENABLE_3PCC_ENVIRONMENT=1.
##
## BW_ENABLE_DIR specifies BroadWorks Directory feature availability state.
##  Value  Operation
##    0    disable
##    1    enable (default)
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (Not supported by J129)
## SET BW_ENABLE_DIR 0
##
## BW_ENABLE_DIR_ENTERPRISE specifies BroadWorks Enterprise directory availability state.
##  Value  Operation
##    0    disable
##    1    enable (default)
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (Not supported by J129)
## SET BW_ENABLE_DIR_ENTERPRISE 0
##
## BW_ENABLE_DIR_ENTERPRISE_COMMON specifies BroadWorks Enterprise Common directory availability state.
##  Value  Operation
##    0    disable
##    1    enable (default)
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (Not supported by J129)
## SET BW_ENABLE_DIR_ENTERPRISE_COMMON 0
##
## BW_ENABLE_DIR_GROUP specifies BroadWorks Group directory availability state.
##  Value  Operation
##    0    disable
##    1    enable (default)
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (Not supported by J129)
```

Copyright Avaya 2019 All rights reserved

```
## SET BW_ENABLE_DIR_GROUP 0
##
## BW_ENABLE_DIR_GROUP_COMMON specifies BroadWorks Group Common directory availability state.
##  Value  Operation
##    0    disable
##    1    enable (default)
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (Not supported by J129)
## SET BW_ENABLE_DIR_GROUP_COMMON 0
##
## BW_ENABLE_DIR_PERSONAL specifies BroadWorks Personal directory availability state.
##  Value  Operation
##    0    disable
##    1    enable (default)
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (Not supported by J129)
## SET BW_ENABLE_DIR_PERSONAL 0
##
## BW_ENABLE_DIR_CUSTOM specifies BroadWorks Custom directory availability state.
##  Value  Operation
##    0    disable
##    1    enable (default)
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (Not supported by J129)
## SET BW_ENABLE_DIR_CUSTOM 0
##
## BW_DIR_ENTERPRISE_DESCRIPTION specifies the display name for BroadWorks Enterprise directory.
##  The default is "Enterprise".
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (Not supported by J129)
## SET BW_DIR_ENTERPRISE_DESCRIPTION "LargeEnterprise"
##
## BW_DIR_ENTERPRISE_COMMON_DESCRIPTION specifies the display name for BroadWorks Enterprise Common directory.
##  The default is "Enterprise Common".
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (Not supported by J129)
## SET BW_DIR_ENTERPRISE_COMMON_DESCRIPTION "DirectoryName"
##
## BW_DIR_GROUP_DESCRIPTION specifies the display name for BroadWorks Group directory.
##  The default is "Group".
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (Not supported by J129)
## SET BW_DIR_GROUP_DESCRIPTION "Sales"
##
## BW_DIR_GROUP_COMMON_DESCRIPTION specifies the display name for BroadWorks Group Common directory.
##  The default is "Group Common".
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (Not supported by J129)
## SET BW_DIR_GROUP_COMMON_DESCRIPTION "SalesTeam"
##
## BW_DIR_PERSONAL_DESCRIPTION specifies the display name for BroadWorks Personal directory.
##  The default is "Personal".
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (Not supported by J129)
## SET BW_DIR_PERSONAL_DESCRIPTION "PersonalList"
##
## BW_DIR_CUSTOM_DESCRIPTION specifies the display name for BroadWorks Custom directory.
##  The default is "Custom".
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (Not supported by J129)
## SET BW_DIR_CUSTOM_DESCRIPTION "CustomDescription"
##
## BW_DIR_ENTERPRISE_EXTENSION specifies the display name for BroadWorks Enterprise directory extension.
##  The default is "BWEntr".
##  This parameter is supported by:
##      J100 SIP R4.0.0.0 and later (Not supported by J129)
## SET BW_DIR_ENTERPRISE_EXTENSION "BWEntrA"
##
```

Copyright Avaya 2019 All rights reserved

BW_DIR_ENTERPRISE_COMMON_EXTENSION specifies the display name for BroadWorks Enterprise Common directory extension.
The default is "BW EnCom".
This parameter is supported by:
J100 SIP R4.0.0.0 and later (Not supported by J129)
SET BW_DIR_ENTERPRISE_COMMON_EXTENSION "BW EnCom1"
##
BW_DIR_GROUP_EXTENSION specifies the display name for BroadWorks Group directory extension.
The default is "BW Group".
This parameter is supported by:
J100 SIP R4.0.0.0 and later (Not supported by J129)
SET BW_DIR_GROUP_EXTENSION "BW GroupA"
##
BW_DIR_GROUP_COMMON_EXTENSION specifies the display name for BroadWorks Group Common directory extension.
The default is "BW GrCom".
This parameter is supported by:
J100 SIP R4.0.0.0 and later (Not supported by J129)
SET BW_DIR_GROUP_COMMON_EXTENSION "BW GrComA"
##
BW_DIR_PERSONAL_EXTENSION specifies the display name for BroadWorks Personal directory extension.
The default is "BW Pers".
This parameter is supported by:
J100 SIP R4.0.0.0 and later (Not supported by J129)
SET BW_DIR_PERSONAL_EXTENSION "BW PersA"
##
BW_DIR_CUSTOM_EXTENSION specifies the display name for BroadWorks Custom directory extension.
The default is "BW Cust".
This parameter is supported by:
J100 SIP R4.0.0.0 and later (Not supported by J129)
SET BW_DIR_CUSTOM_EXTENSION "BW CustA"
##
##
##
96xx/96x1/H1xx/J129/J139/J169/J179 SIP TELEPHONE SETTINGS
##
##
WAIT_FOR_CALL_OPERATION_RESPONSE specifies the time in seconds before providing a response for user initiated call operation.
This parameter is applicable to all server environments (Aura, IP Office and 3PCC).
When user goes off-hook, then phone sends an invite. If there is no response from the SIP proxy for the number of seconds defined in WAIT_FOR_CALL_OPERATION_RESPONSE,
it will result in a user notification that the operation is in progress but is delayed.
Value range is 1-4. The default is 3.
This parameter is supported by:
J100 SIP R4.0.0.0 and later
SET WAIT_FOR_CALL_OPERATION_RESPONSE 2
##

Changed parameters.

###################### DHCP SETTINGS ######################
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 H.323 R6.7 and later

Copyright Avaya 2019 All rights reserved

J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and later, J139 SIP R3.0.0.0 and later
J100 SIP R4.0.0.0 and later: REUSETIME specifies the number of seconds that DHCPV4 or DHCPv6 discovery will be attempted before either:
reusing the previously cached value of IPv4 address (and associated address information) that the Phone had the last time successfully
registered with a call server, if such an address is available, or continue discovery DHCPv6 server: IPv6 does not support reuse,
so there is no corresponding parameter to IPv4's REUSE_IPADD.
While reusing an address, DHCPV4 will enter the extended rebinding state described for DHCPSTD.
A value of zero means that DHCP or DHCPv6 will be tried forever (i.e., no reuse).
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

################# SERVER SETTINGS (SIP) ################
SIP_CONTROLLER_LIST specifies a list of IPv4 SIP controller designators,
separated by commas without any intervening spaces.
The list is used on IPv4-only and dual mode phones (if SIP_CONTROLLER_LIST_2 is not provided).
Each controller designator has the following format:
host[:port][;transport=xxx]
host is an IP address in dotted-decimal (DNS name format is not supported unless stated otherwise below).
[:port] is an optional port number.
[;transport=xxx] is an optional transport type where xxx can be tls, tcp or udp.
If a port number is not specified a default value of 5060 for TCP and UDP or 5061 for TLS is used.
If a transport type is not specified, a default value of tls is used.
The value can contain 0 to 255 characters; the default value is null ("").
This parameter is supported by:
J129 SIP R1.0.0.0 (or R1.1.0.0); J100 SIP R2.0.0.0 and later; J139 SIP R3.0.0.0 and later; DNS name format is supported for 3PCC environment only.
For 3PCC environment, only one SIP controller is supported.
J100 SIP R4.0.0.0 and later; used on dual mode phones if SIP_CONTROLLER_LIST_2 is not provided.
When 3PCC_SERVER_MODE = 1 (a BroadSoft server), SIP_CONTROLLER_LIST should contain one sip controller entry and host should be an FQDN (DNS name format).
The FQDN would resolve to primary and alternate servers to support redundant configuration.
When 3PCC_SERVER_MODE = 0 (a generic SIP server), SIP_CONTROLLER_LIST may contain one or two sip controller entries (to support redundant configuration).
“host” of sip controller entry could be an FQDN(DNS name format) or an IP address. If FQDN is provided, it will resolve to one primary server.
IPv6 is not supported for 3PCC environment. In 3PCC environment, there is no support for resolving an FQDN to an IPv6 address in the SIP_CONTROLLER_LIST or SIP_CONTROLLER_LIST_2.
IPv6 is supported for Aura environment and in Aura there is no support for FQDN yet (only IP addresses can be configured).
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.
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

Copyright Avaya 2019 All rights reserved

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 on IPv6-only phones to provide the list of SIPv6 servers.
SIPv4 servers are ignored in IPv6-only mode. 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. Dual mode phones use SIP_CONTROLLER_LIST if SIP_CONTROLLER_LIST_2 is not provided.
SIP_CONTROLLER_LIST_2 should only be used if IPv6 addresses (FQDN is not supported) may be used for SIP signaling.
SIP_CONTROLLER_LIST_2 should not be used if FQDN (DNS name format) is used for sip controllers.
##
This parameter is supported by:
J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later, J139 SIP R3.0.0.0 and later
96x1 SIP R7.1.0.0 and later
Example:
Dual mode SIP controllers:
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}"
IPv6-only mode SIPv6 controllers:
SET SIP_CONTROLLER_LIST_2 "[2007:7::5054:ff:fe35:c6e]:5060;transport=tcp,[2007:7::5054:ff:fe80:d4b0]:5060;transport=tcp"
##
################## DEVICE ENROLLMENT SERVICE (DES) ##################
##
DES_STAT Specifies if DES discovery is to be attempted during the boot process if there is no configuration file server provisioned on the phone.
Value Operation
0 DES discovery is disabled and can only be restored with Reset to Defaults
1 DES discovery is disabled
2 DES discovery is enabled (default); user prompt is displayed for end user to enforce "DES" or not.
3 DES discovery is enforced without dependency on user to select "yes" on the prompt appears after reboot.
This parameter is supported by:
J100 SIP R2.0.0.0 and later, J139 SIP R3.0.0.0 and later, value 3 is supported by J100 SIP R4.0.0.0 and later
Avaya Vantage Devices SIP R1.1.0.0 and later; if FILE_SERVER_URL/HTTPSRVR/TLSSRVR are received from DHCP/LLDP/UI/configuration file/AADS then DES will not be activated.
No support for user prompt which can enforce DES or not. Value 3 is not supported.
SET DES_STAT 1

###
IPv6 related settings are applicable for 96x1 H.323 R6.0 and later, J169/J179 H.323 R6.7 and later, 96x1 SIP R7.1.0.0 and later, J169/J179 SIP R1.5.0 and J100 SIP R2.0.0.0 and later.
DHCPSTAT

Copyright Avaya 2019 All rights reserved

Valid Values

1 run DHCPv4 only (IPv4only-mode, if no own IPv6 address is programmed statically), Default.

2 run DHCPv6 only (IPv6only-mode, if no own IPv4 address is programmed statically)

3 run both DHCPv4 & DHCPv6 (dual-stack mode)

Description

Specifies whether DHCPv4, DHCPv6, or both will be used in case IPV6STAT has enabled IPv6 support generally

Example : Setting dual stack mode

SET DHCPSTAT 3

This parameter is supported by:

J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later, J139 SIP R3.0.0.0 and later
For J100 SIP R4.0.0.0 and later - Specifies whether DHCPv6 is enabled or disabled. DHCPSTAT is used in dual (IPV6STAT=1) and IPv6-only (IPV6STAT=2) modes.
NOTE: DHCPv4 is always enabled in IPv4 only and dual mode. DHCPv4 is disabled in IPv6 only mode.
Value 1: disable DHCPv6 client, (For IPV6STAT=1 (IPv6 enabled) & "Use SLAAC=No" (SLAAC disabled): IPv4only-mode, if no Phone(v6) IPv6 address is programmed statically
For IPV6STAT=2 (IPv6 only) & "Use SLAAC=No" (SLAAC disabled): Phone(v6) address has to be set manually).
Value 2,3: enable DHCPv6 client (dual-stack mode).
The default value is 3.

J169/J179 H.323 R6.7 and later

96x1 SIP R7.1.0.0 and later; Value 1 as described above, Value 2/3 - run both DHCPv4 & DHCPv6

96x1 H.323 R6.0 and R6.0

SET DHCPSTAT 1

IPV6STAT

Valid Values
0 IPv6 will not be supported (IPv4 only mode).
1 Dual mode (IPv4 and IPv6) will be supported.
2 IPv6 only mode (only supported by J100 SIP 4.0.0.0 and greater)

Description

Specifies whether IPv6 will be supported

This parameter is supported by:

J169/J179 H.323 R6.7 and later
J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later, J139 SIP R3.0.0.0 and later (Default is 0), J100 SIP R4.0.0.0 and later (default is 1).

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.
The single IPv6 mode phone ignores SIGNALING_ADDR_MODE and SIP_CONTROLLER_LIST and selects the SIP controller's IPv6 addresses from SIP_CONTROLLER_LIST_2.

This parameter is supported by:

J169/J179 SIP R1.5.0; J100 SIP R2.0.0.0 and later, J139 SIP R3.0.0.0 and later

96x1 SIP R7.1.0.0 and later

Copyright Avaya 2019 All rights reserved

Example:
SET SIGNALING_ADDR_MODE 4

#################### COUNTRY AND DATE SETTINGS ####################
Time Format
Specifies the format of the time displayed in the phone.
0 for am/pm format (Default)
1 for 24h format
The TIMEFORMAT configured in the settings file is used in the following cases:
1. The phone is not registered to Avaya Aura Session Manager
2. If the phone is registered to Avaya Aura Session Manager AND
A. there is no information stored for the timeformat for this specific user (first time login of this user)
AND
B. there is no support of "Profile Settings" in the "Endpoint Template" (which is supported by SMGR 6.3.8 and up).
This parameter is supported by:
J129 SIP R1.0.0.0 (or R1.1.0.0), J100 SIP R2.0.0.0 and later, J139 SIP R3.0.0.0 and later - The TIMEFORMAT can also be set from the phone's local menu
independent of the environment (3PCC, Aura, IP Office). The TIMEFORMAT will be used in the above cases until user manually changes the value.
96x1 SIP R6.0 and later
H1xx SIP R1.0 and later
Avaya Vantage Devices SIP R1.0.0.0 and later (up to R1.0.0.0 build 2304).
SET TIMEFORMAT 1

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.