Installing and Administering Avaya J100 Series SIP IP Phones in Open SIP

Release 4.0.11
Issue 1
February 2022

© 2020-2022, Avaya Inc.
All Rights Reserved.

Note

Using a cell, mobile, or GSM phone, or a two-way radio in close proximity to an Avaya IP telephone might cause interference.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“**Hosted Service**” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Shrinkwrap License (SR). End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Regulatory Statements

Australia Statements

Handset Magnets Statement:

Danger:

The handset receiver contains magnetic devices that can attract small metallic objects. Care should be taken to avoid personal injury.

Industry Canada (IC) Statements

RSS Standards Statement

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. L'appareil ne doit pas produire de brouillage, et
2. L'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Radio Transmitter Statement

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Radiation Exposure Statement

This equipment complies with FCC & IC RSS102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Cet équipement est conforme aux limites d'exposition aux rayonnements ISEDétablies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Japan Statements

Class B Statement

This is a Class B product based on the standard of the VCCI Council. If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。　　VCCI－B

Denan Power Cord Statement

Danger:

Please be careful of the following while installing the equipment:

- Please only use the connecting cables, power cord, and AC adapters shipped with the equipment or specified by Avaya to be used with the equipment. If you use any other equipment, it may cause failures, malfunctioning, or fire.
- Power cords shipped with this equipment must not be used with any other equipment. In case the above guidelines are not followed, it may lead to death or severe injury.

警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

- 接続ケーブル、電源コード、AC アダプタなどの部品は、必ず製品に同梱されております添付品または指定品をご使用ください。添付品指定品以外の部品をご使用になると故障や動作不良、火災の原因となることがあります。
- 同梱されております付属の電源コードを他の機器には使用しないでください。上記注意事項を守らないと、死亡や大怪我など人身事故の原因となることがあります。

México Statement

The operation of this equipment is subject to the following two conditions:

1. It is possible that this equipment or device may not cause harmful interference, and
2. This equipment or device must accept any interference, including interference that may cause undesired operation.

La operación de este equipo está sujeta a las siguientes dos condiciones:

1. Es posible que este equipo o dispositivo no cause interferencia perjudicial y
2. Este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

Brazil Statement

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados

Power over Ethernet (PoE) Statement

This equipment must be connected to PoE networks without routing to the outside plant.

Taiwan Low Power Radio Waves Radiated Devices Statement

取得審驗證明之低功率射頻器材，非經核准，公司、商號或使 用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應 立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理 法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及 醫療用電波輻射性電機設備之干擾。

U.S. Federal Communications Commission (FCC) Statements

Compliance Statement

The changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interferences that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designated to provide reasonable protection against harmful interferences in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause

harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interferences to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment . This equipment should be installed and operated with minimum distance of 8 in or 20 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

ENERGY STAR® compliance statement

As an ENERGY STAR partner, Avaya Inc. has determined that this product meets the ENERGY STAR guidelines for energy efficiency. Information on the ENERGY STAR program can be found at www.energystar.gov. ENERGY STAR and the ENERGY STAR mark are registered trademarks owned by the U.S. Environmental Protection Agency.

EU Countries

This device when installed complies with the essential requirements and other relevant provisions of the EMC Directive 2014/30/EU, Safety LV Directive 2014/35/EU, and Radio Equipment Directive 2014/53/EU. A copy of the Declaration may be obtained from https://support.avaya.com or Avaya Inc., 2605 Meridian Parkway Suite 200. Durham, NC 27713 USA.

WiFi transmitter

- Frequencies for 2412-2472 MHz, transmit power: < 20 dBm
- Frequencies for 5180-5240 MHz, transmit power: < 20 dBm

BT transmitter

- Frequencies for 2402-2480 MHz, transmit power: < 6.0 dBm

General Safety Warning

- Use only the Avaya approved Limited Power Source power supplies specified for this product.
- Ensure that you:
  - Do not operate the device near water.
  - Do not use the device during a lightning storm.
  - Do not report a gas leak while in the vicinity of the leak.
  - For Accessory Power Supply in Avaya J100 Series IP Phones– Use Only Limited Power Supply Phihong Technology Co. Ltd. Model: PSAC12R-050, Output: 5VDC, 2.4A.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

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

Device Usage Consent

By using the Avaya device you agree that Avaya, from time to time, may collect network and device data from your device and may use such data in order to validate your eligibility to use the device.

Contents

Chapter 1: Introduction 13
Purpose 13
Change history 13
Chapter 2: Avaya J100 Series IP Phones overview 15
J100 Series IP Phone models 15
Secondary display 16
Expansion modules 16
Wi-Fi Module 18
Hardware specifications 18
Power specifications 21
Supported codecs 23
Chapter 3: Initial setup and connectivity 24
Initial setup checklist 24
Installing the wireless module 25
Wireless Module configuration 28
Wall mounting Avaya J100 Series IP Phones 28
Wall mounting Avaya J100 Expansion Module 30
Software installation 32
Identifying the device type during phone boot-up 32
Automatic phone provisioning 32
Automatic phone provisioning using Device Enrollment Services 33
Entering the provisioning details 34
Provisioning server mutual authentication support 34
Manual phone provisioning 35
Prerequisites 35
Phone administration methods 36
Downloading and saving the software 37
Modifying the settings file 39
Installation checklist 39
Phone initialization 40
Cloud configuration 41
Configuration through a cloud server 41
Phone setup process on a cloud server 41
Settings file contents on a cloud server 42
MAC address file contents on a cloud server 42
Chapter 4: Servers, VLAN, and IP configuration 44
Server configuration 44
Setting up a provisioning server 44
Provisioning Server configuration 45

SNTP server configuration ... 47
SNTP Parameters ... 47
DHCP server configuration ... 49
Setting up a DHCP server ... 49
Configuration through DHCP ... 50
Setting up a DHCP server ... 50
DHCP options ... 51
DHCP site-specific option ... 55
Configuration through LLDP ... 57
LLDPDU transmitted by the phones ... 58
TLV impact on system parameter values ... 59
Automatic phone provisioning using Device Enrollment Services ... 61
Virtual LAN (VLAN) ... 61
VLAN separation ... 62
Configuring an external switch port ... 64
Exceptions to the VLAN forwarding rules ... 65
Special considerations ... 65
VLAN parameters ... 65
TCP and UDP ports ... 69
Received packets (destination = SIP phone) ... 69
Transmitted packets (source = SIP phone) ... 70
Session Traversal Utilities for NAT overview ... 71
STUN parameters ... 72
IPv4 and IPv6 ... 75
Configuring IPv4 from the phone menu ... 75
Configuring IPv4 from the web interface ... 76
Configuring a DHCP server in the dual and IPv6-only environments ... 76
IPv6 configuration ... 77
Configuring IPv6 from the phone menu ... 79
Configuring IPv6 from the web interface ... 80
IPv6 limitations ... 81
Microsoft® Exchange account integration ... 81
Microsoft Exchange account integration configuration parameters ... 81
Chapter 5: Open SIP operation modes ... 86
Configuring an Open SIP operation mode through the settings file ... 86
Configuring an Open SIP operation mode through the web interface ... 87
Broadsoft configuration ... 88
BroadSoft server mode ... 88
Broadworks topology ... 89
Broadsoft Device Management ... 90
Chapter 6: Phone configuration ... 93
Configuring the phone using Administration menu ... 93
Accessing the Admin menu during phone startup ... 94

Accessing the Admin menu after log in..... 94
Accessing the Ethernet IPv4 settings..... 95
Signaling protocol..... 97
Using the debug mode..... 98
Setting the Ethernet interface control..... 99
Group identifier..... 100
Setting event logging..... 101
Setting the dial plan..... 102
Restarting the phone..... 104
Configuring Wi-Fi using phone UI..... 104
Configuring SIP settings..... 105
Setting Site Specific Option Number (SSON)..... 107
Accessing the View menu..... 108
Checking the phone update status..... 110
Checking the phone update policy..... 111
IEEE 802.1X overview..... 111
Updating phone settings and firmware..... 113
Resetting system values..... 114
Configuring the phone using the web interface..... 115
Enabling access to web interface of the phone..... 116
Logging in to the phone web interface..... 117
Logging out of the phone web interface..... 118
Password for the phone web interface..... 118
Changing the default phone web interface password..... 119
Web interface screen layout..... 119
Changing the phone web interface password..... 120
Viewing the status of the phone configuration..... 120
Configuring network settings..... 124
Configuring IP settings..... 132
Configuring QoS settings..... 138
Configuring NAT and STUN settings..... 139
Configuring Web Server settings..... 141
Configuring SIP settings..... 143
Configuring Settings..... 155
Configuring date and time..... 185
Configuring management settings..... 187
Changing the password of the phone Administrator menu..... 190
Debugging..... 191
Capturing the phone network traffic..... 195
Configuring certificates..... 196
Configuring Environment Settings..... 200
Configuring Background and Screen Saver of the Phone..... 201
Configuring Calendar of the phone..... 203

Configuring Multicast Paging 205
Setting Pre-configuration of keys 207
Configuring softkey sets 209
Configuring Shared Lines 214
Restarting your phone through web interface 216
Resetting the phone to Default 216
Configuring the phone using the settings file 217
Contents of the settings file 218
Modifying the Settings file 219
Phone display language 219
Pre-configuration of keys 221
Pre-configuration of keys parameter 221
Phonekey Labels 223
Viewing PHONEKEYLIST parameter details 223
Soft key configuration 224
Configuration of soft key parameter for primary call appearance state 226
Configuration of soft key parameters for Shared Call Appearance and Bridged Line Appearance states 235
Configuration of soft key parameter for Busy lamp field call appearance states 245
Chapter 7: Feature and application configuration 250
Application configuration 252
Calendar 252
Contacts list 254
Recents 256
Ringtones 257
Feature configuration 262
Active call shortcut keys 262
Adjusting the Sidetone level 263
Anywhere and Mobility 265
Avaya Spaces Calendar integration 266
BroadWorks advance call control 269
BroadSoft XSI support 269
Busy Lamp Field 271
BroadWorks Directory 279
BroadWorks Call center 282
Broadsoft Call recording indicator 287
Call Park 288
Call decline policy 288
Call forwarding on a generic SIP server 288
Call forwarding on Broadsoft 290
Call Waiting 291
Centralized call logs 291
Centralized personal contacts 292

Digit mapping 292
Downloadable directory 296
Display name configuration 297
Distinctive Ringing 298
Distinctive Alert Waiting Tone 298
Dynamic Park and Page 299
Force HTTP/HTTPS provisioning server credentials 301
Flexible Seating 304
Group Paging 305
Long-term acoustic protection 305
LDAP Directory 306
Off-hook alert 314
Multicast Paging 315
Prioritization of codecs 318
Push 319
Push-To-Talk 321
Phone screen width 322
Shared Lines 324
Scrolling mode 332
Shared Parking 333
Selection of a higher priority line after ending a call 334
Server-initiated Update 335
Simultaneous Ring Personal 336
USB Headset 336
USB Flash drive 337
USB keyboard 339
WML browser 340
Voicemail 342
Visual voicemail 343

Chapter 8: Security configurations 345
Security overview 345
Locking and unlocking the phone 346
Phone lock configuration parameter 346
Access control and security 347
FIPS mode 348
FIPS mode parameter 349
Geographical restrictions on encryption 350
Certificate management 350
Identity certificates 351
Trusted certificates 352
OCSP trust certificates 352
Key Usage check for security certificates 353
Key Usage checking configuration 353

Parameter configuration for secure installation 353
Chapter 9: Data Privacy Controls Addendum 356
Purpose 356
Data categories containing personal data (PD) 356
Personal data human access controls 357
Personal data programmatic or API access controls 357
Personal data at rest encryption controls 358
Personal data in transit encryption controls 358
Personal data retention period controls 359
Personal data export controls and procedures 359
Personal data view, modify, delete controls and procedures 360
Personal data pseudonymization operations statement 361
Data privacy and secure data processing 361
Secure mode 361
Configuring secure mode parameter 362
Data privacy 362
Secure Syslog 364
Secure Syslog parameters 364
Geographical restrictions on encryption 365
Chapter 10: SIP server redundancy configuration 366
SIP server redundancy 366
Redundancy in generic Open SIP 366
Redundancy in a Broadsoft environment 368
Redundancy in a Netsapiens environment 370
DNS resolution 372
User experience when redundancy is configured 373
User interface notification parameter 373
Chapter 11: Backup and restore 374
Backup and restore process 374
Chapter 12: Maintenance 376
Phone installation - best practices 376
Device upgrade process 376
Periodic check for software and settings update 377
Periodic check of software and settings update configuration 377
Avaya J100 Expansion Module upgrade 381
Upgrading the expansion module 382
Post installation checklist 382
Chapter 13: Resources 384
Documentation 384
Finding documents on the Avaya Support website 384
Avaya Documentation Center navigation 384
Viewing Avaya Mentor videos 386
Support 386

Appendix A: Customizable parameters 387
List of configuration parameters 387
List of Wi-Fi configuration parameters 540
Downloadable directory syntax 545
Soft key parameter values 546
PHONEKEY parameter values 552
BLF configuration modes 556
Nesting of WML elements 558
WML syntax specifications for Avaya J100 Series IP Phones 559
Appendix B: Public CA Certificates 574
Public CA Certificates 574
Appendix C: Network progress tones overview 582

Chapter 1: Introduction

Purpose

This document focuses on preparing Avaya J100 Series IP Phones for installation, initial administration, and administration tasks.

This document is intended for the administration engineers or support personnel who install, administer, and maintain Avaya J100 Series IP Phones.

The administration engineers or the support personnel must have the following knowledge and skills:

Knowledge

- DHCP
- SIP
- 802.1x and VLAN

Skills

Administering and configuring:

- DHCP server
- HTTP or HTTPS server
- Microsoft Exchange Server

Change history

Issue	Date	Summary of changes
Release 4.0.9	April 2021	• Updated “Feature and application configuration” chapter • Updated "Avaya J100 Series IP Phones overview" chapter • Updated "Phone configuration" chapter • Updated Appendix

Table continues…

Issue	Date	Summary of changes
Release 4.0.10	July 2021	• Updated “Feature and application configuration” chapter • Updated "Servers, VLAN, and IP configuration" chapter • Updated "Open SIP operation modes" chapter • Updated "Phone configuration" chapter • Updated "Security configurations" chapter • Updated Appendix
Release 4.0.11	February 2022	• Updated “Feature and application configuration” chapter • Updated "Phone configuration" chapter • Updated "Security configurations" chapter • Updated Appendix

Chapter 2: Avaya J100 Series IP Phones overview

Avaya J100 Series IP Phones provide a range of applications and features for unified communications. The phones leverage the enterprise IP network and eliminate the need of a separate voice network. The phones offer superior audio quality with the amplified handsets and customization with low power requirements in a Session Initiation Protocol (SIP) environment.

Avaya J100 Series IP Phones work with BroadSoft, Metaswitch, FreeSWITCH, Netsapiens, Asterisk, RingCentral, Avaya Cloud Office™, and Generic Open SIP environments to provide a flexible architecture where you can:

- Make conference calls more efficiently and enhance customer interactions with high-quality audio.
- Gain access to information quickly through easy-to-read high-resolution displays.
- Create a survivable, scalable infrastructure that delivers reliable performance and flexible growth as business needs change.
- Increase performance by deploying Gigabit Ethernet within your infrastructure.
- Reduce energy costs by using efficient Power-over-Ethernet (PoE) including sleep mode, which lowers energy consumption significantly.
- Enhance audio quality by using amplified handset mode.

J100 Series IP Phone models

Phone model	Description
J129 IP Phone	A phone with a monochrome display that supports single line call appearance.
J139 IP Phone	A phone with a color display that has four lines/feature/application buttons. The primary display is scrollable that supports up to 96 lines/features/applications.

Table continues…

Phone model	Description
J159 IP Phone	A phone with a Primary color display that has four lines/features/applications buttons. The Primary display is scrollable that supports up to 96 lines/features/applications. A Secondary color display has 6 lines/features/applications buttons. The Secondary display is pageable that supports up to 24 lines/features/applications.
J169 IP Phone	A phone with a grayscale display that supports eight lines/features/applications buttons. The Primary display is scrollable that supports up to 96 lines/features/applications. The phone can also support up to three button modules, each supporting 24 lines/features/applications buttons.
J179 IP Phone	A phone with a color display that supports eight lines/features/applications buttons. The Primary display is scrollable that supports up to 96 lines/features/applications. The phone can also support up to three button modules, each supporting 24 lines/features/applications buttons.
J189 IP Phone	A phone with a Primary color display that supports 10 lines/features/applications buttons. The Primary display is scrollable, supporting up to 96 line/feature/applications. A Secondary color display that supports 6 lines/features/applications buttons. The Secondary display is pageable supporting up to 24 lines/features/applications. The phone can also support up to two button modules, each supporting 24 lines/features/applications buttons.

Secondary display

Avaya J159 IP Phone and Avaya J189 IP Phone have a secondary display for additional call appearances and feature or application display.

It has six lines of four-page display that provides 24 additional lines for incoming calls, outgoing calls, auto-dialing, and calling features. It displays the dedicated view for keys 25-48. You can switch between the pages using the left and right keys.

Expansion modules

On , the number of call appearances and feature buttons can be extended with the Avaya J100 Expansion Module (JEM24) and JBM24 Button Module (JBM24).

Avaya J100 Expansion Module provides 72 additional lines, and the JBM24 Button Module provides 24 additional lines for incoming calls, outgoing calls, auto-dialing, and calling features.

You can connect up to three button modules to Avaya J169/J179 IP Phones and up to two expansion modules to Avaya J189 IP Phone. Each module can be placed in stand and wall mount positions together with the phone.

Important:

Avaya J100 Expansion Module does not support Hot plugging. Connect all the expansion modules to the phone before connecting the phone to a power source.

The following table shows the number of button modules attached to the phone and the corresponding number of lines available on the Avaya J100 Expansion Module or JBM24 Button Module:

Model	Attached Button module1	Attached Button module2	Attached Button module3	Call lines/ Features	Switching between pages
Avaya J169/ J179 IP Phone	Yes	Yes	Yes	24 on each page	Yes
Avaya J189 IP Phone	Yes	Yes	No	24 on each page	No

Avaya J189 IP Phone supports up to two Avaya J100 Expansion Modules. The following power limitations apply when you connect the JEM24 button modules to the phone:

Power adapters	USB power	1 JEM24 modules	2 JEM24 modules
PoE (Side switch position L)	USB Type-A power limited to 100mA	Not supported	Not supported
PoE (Side switch position H)	USB Type-A and USB Type-C	Supported, with USB Type-A and Type-C port shared power limited to 900mA	Supported,with USB Type-A and Type-C port shared power limited to 500mA
5V power adapter	USB Type-A and USB Type-C	Supported, with USB Type-A and Type-C port shared power limited to 900mA	Supported,with USB Type-A and Type-C port shared power limited to 500mA

Avaya J189 IP Phone can support two JEM24 module with USB headset USB Type-A and USB Type-C working.

- If the USB headset uses a USB Type-C cable, the POE side switch should be set to H position or use a 5v adapter.
- If the USB headset uses a USB Type-A cable, it works with a USB-A port, and the power consumption is within the port limit.

Note:

When an Avaya J100 Expansion Module is attached to the Avaya J169 IP Phone, the display screen changes to gray scale.

Wi-Fi Module

The Avaya J100 Wireless Module enables the phone to connect to a wireless network. The phone displays the Wi-Fi status icon when the Wi-Fi network is in use. If the phone loses connection to one Wi-Fi network, it continues to operate with another configured wireless network or an Ethernet network. If the phone is connected to Ethernet switch and the Ethernet link goes down, a pop-up message notifies the user to change network connectivity to Wi-Fi.

Note:

PC port is disabled when a Wi-Fi network is used.

The wireless module is an optional component, and you can order this module separately. The Avaya J100 Wireless Module provides Wi-Fi and Bluetooth connectivity to the following phone models:

Model	Wi-Fi support from software version	Bluetooth support from software version
Avaya J129 IP Phone	2.0.0 and later	Not supported
Avaya J179 IP Phone	2.0.0 and later	4.0.0 and later
Avaya J159 IP Phone	4.0.4 and later	4.0.8 and later
Avaya J189 IP Phone	4.0.6.1 and later	4.0.6.1 and later

Hardware specifications

Avaya J100 Series IP Phones support the following hardware specifications:

Device dimensions

The dimensions are with phone stand in high position and wall mount.

Model	Phone stand in high position (Wide x Deep x Tall in mm)	Phone dimensions in wall mount (Wide x Deep x Tall in mm)
J129	156 x 170 x 175	156 x 100 x 198
J139	179 x 170 x 177	179 x 100 x 219
J159	185 x 170 x 224	185 x 100 x 225
J169	187 x 175 x 183	187 x 100 x 225
J179	187 x 175 x 183	187 x 100 x 225
J189	227 x 179 x 199	227 x 100 x 244
JBM24	89 x 175 x 183	89 x 100 x 225
JEM24	115 x 175 x 140	115 x 100 x 175

Display and Call appearances

Model	Display (pixels)	Display type	Call appearances
J129	2.3”, 128 x 32	Monochrome	1
J139	2.8”, 320 x 240	Color	4
J159	2.8”, 320 x 240 primary display 2.4”, 240 x 320 secondary display	Color	4 on the primary display 24 on the secondary display
J169	3.5”, 320 x 240	Grayscale	8
J179	3.5”, 320 x 240	Color	8
J189	5”, 800 x 480 primary display 2.4”, 240 x 320 secondary display	Color	10 on the primary display 24 on the secondary display
JBM24	3.3”, 160 x 320	Grayscale	NA
JEM24	4.3”, 272 x 480	Grayscale and color	NA

Ethernet, Wi-Fi, and Bluetooth- specifications

Model	Ethernet switch	Wi-Fi support	Bluetooth support
J129	Dual 10/100	Yes, with an optional module	No
J139	Dual 10/100/1000	No	No
J159	Dual 10/100/1000	Yes, with an optional module	Yes, with an optional module
J169	Dual 10/100/1000	No	No
J179	Dual 10/100/1000	Yes, with an optional module	Yes, with an optional module
J189	Dual 10/100/1000	Yes, with an optional module	Yes, with an optional module
JBM24	NA	NA	NA
JEM24	NA	NA	NA

Handset and Headset- specifications

Model	Wired handset (HAC)	Amplified handset mode	Wired headset
J129	Yes	Yes, with 20dB of gain	No
J139	Yes	Yes, with 20dB of gain	Yes
J159	Yes	Yes, with 20dB of gain	Yes

Table continues…

Model	Wired handset (HAC)	Amplified handset mode	Wired headset
J169	Yes	Yes, with 20dB of gain	Yes
J179	Yes	Yes, with 20dB of gain	Yes
J189	Yes	Yes, with 20dB of gain	Yes
JBM24	NA	NA	NA
JEM24	NA	NA	NA

Power and USB support

Model	PoE[1]	Optional DC power	USB port
J129	Yes	Yes[2]	No
J139	Yes	Yes	No
J159	Yes	Yes	Yes
J169	Yes	Yes	No
J179	Yes	Yes	No
J189	Yes	Yes	Yes
JBM24	NA	NA	No
JEM24	NA	NA	No

Other specifications

Model	Dual color call indicator	Soft keys call control	Expansion module capable
J129	0	3	No
J139	4	4	No
J159	4	4	No
J169	8	4	Yes, 3 modules
J179	8	4	Yes, 3 modules
J189	10	4	Yes, 2 modules
JBM24	0	NA	NA
JEM24	24	NA	NA

[1] PoE can be supplied from one of the following:

- Data switch
- in-line PoE injector

[2] Optional DC power is available in J129D03A and later hardware models. J129D01A and J129D02A do not support optional DC power.

Power specifications

Avaya J100 Series IP Phones can be powered using Power over Ethernet (PoE) or a 5V DC adapter. You must purchase the power adapter separately.

Avaya J100 Series IP Phones are ENERGY STAR® compliant.

Important:

- Avaya J129 IP Phone, Avaya J159 IP Phone, Avaya J179 IP Phone, and Avaya J189 IP Phone support the wireless module.
- Avaya J139 IP Phone is a Class 1 device and does not support peripherals.
- Avaya J159 IP Phone and Avaya J189 IP Phone support an USB device.
- Avaya J169 IP Phone supports three JBM24 Button Modules or two Avaya J100 Expansion Modules on PoE. For additional button modules, use 5V DC power adapter.
- Avaya J179 IP Phone supports two JBM24 Button Modules or one Avaya J100 Expansion Module on PoE. For additional button modules, use 5V DC power adapter.

  Note:

  The simultaneous connection of JBM24 Button Module and Avaya J100 Expansion Module is not supported.
- Avaya J189 IP Phone supports two Avaya J100 Expansion Modules, set the sideswitch to H on PoE or use a 5V adapter.

  Note:

  The connection of JBM24 Button Module is not supported.
- If you are using a power adapter, disable PoE on the Ethernet connection.

The following table provides the LLDP power measurement of the phones, adjuncts, and peripherals.

Phone model	Avaya standard power measurements (in Watts)			Energy Star (in Watts)
	Conservation	Typical	Maximum	Standby
J129	1.26	1.31	1.64	1.04
J139	1.40	1.67	2.24	1.55
J159	1.75	2.32	3.03	2.04
J169	1.72	1.84	2.34	1.85
J179	1.74	2.10	2.71	1.85
J189	2.32	2.91	3.93	1.92
JBM24	0.19	0.69	1.35	NA
JEM24	1.70	1.90	2.00	NA

Table continues…

Phone model	Avaya standard power measurements (in Watts)			Energy Star (in Watts)
	Conservation	Typical	Maximum	Standby
Wi-Fi/BT module	0.90	0.90	0.90	NA
USB device (PoE slide switch in L position)	0.5	0.5	0.5	NA
USB device (PoE slide switch in H position)	1.25	1.25	1.25	NA

The power requirements of the phone vary depending on the connected peripherals. The following table provides the correlation between the connected peripherals and power requirements.

Phone model	PoE Class
J129	• IEEE 802.3af PoE Class 1 device.
J139	• IEEE 802.3af PoE, Class 1 device.
J159	• IEEE 802.3af PoE Class 1, PoE Slide switch in L position, without a wireless module and USB device with parameter USB power value set to either 0, 1 or 3. • IEEE 802.3af PoE Class 2, PoE Slide switch in H position, with a wireless module, USB device, or a wireless module together with USB device.
J169	• IEEE 802.3af PoE Class 1 without a button module. • IEEE 802.3af PoE Class 2 with a button module.
J179	• IEEE 802.3af PoE Class 1 without a wireless module or a button module. • IEEE 802.3af PoE Class 2 for one or more button modules, a wireless module, or a wireless module together with one or more button modules. **Note:** Use 5V DC adapter if you simultaneously connect a wireless module along with one or more button modules of any model.
J189	• IEEE 802.3af PoE Class 2, PoE slide switch in L position with a wireless module. • IEEE 802.3af PoE Class 3, PoE slide switch in H position, one JEM24 module supported with USB Type A and Type C port shared power limited to 900mA.Two JEM24 with USB Type A and Type C port shared power limited to 500mA.

Supported codecs

Avaya J100 Series IP Phones supports the following codecs:

Models	J129	J139	J159	J169	J179	J189
Codecs	• G.711a • G.711µ • G.729 • G.729a • G.729ab • G.726 • G722 • OPUS	• G.711a • G.711µ • G.729 • G.729a • G.729ab • G.726 • G722 • OPUS	• G.711a • G.711µ • G.729 • G.729a • G.729ab • G.726 • G722 • OPUS	• G.711a • G.711µ • G.729 • G.729a • G.729ab • G.726 • G722 • OPUS	• G.711a • G.711µ • G.729 • G.729a • G.729ab • G.726 • G722 • OPUS	• G.711a • G.711µ • G.729 • G.729a • G.729ab • G.726 • G722 • OPUS • OPUS Superwideband

Note:

Codecs support packet loss concealment, jitter buffer where applicable. Full duplex acoustic echo cancellation is active on all transducers

Chapter 3: Initial setup and connectivity

Initial setup checklist

No.	Task	Reference	✔
1	Examine the contents of the shipping package to make sure all the relevant components are available. Avaya J100 Series IP Phones ship in a box containing the IP Phone, handset with a cord, dual-position phone stand, and regulatory/safety sheet. **Note:** An Ethernet cable is not included in the package and must be sourced separately.	*Avaya J100 Series IP Phone Overview and Specifications*	
2	Read and understand the regulatory/ safety sheet provided with the shipping. Download all the relevant documentation for the phone from the Avaya support website.	https://support.avaya.com/documents/	
3	(Optional) Install the wireless module on the phone. **Note:** The wireless module is supported only by Avaya J129 IP Phone, Avaya J159 IP Phone, Avaya J179 IP Phone, and Avaya J189 IP Phone.	Installing the wireless module on page 25	
4	Assemble the phone by connecting handset, and inserting the phone stand into the slots at the back panel of the phone.		

Table continues…

No.	Task	Reference	✔
5	(Optional) Attach the button module to the phone. **Note:** JBM24 Button Module and Avaya J100 Expansion Module are supported only by Avaya J169/J179 IP Phone and Avaya J189 IP Phone.	Expansion modules on page 16	
6	Read and understand the requirement of the open SIP server that you are using to configure the Avaya J100 Series IP Phones.	Open SIP operation modes on page 86	
7	Determine the phone provisioning process required for the open SIP server you are using to configure the Avaya J100 Series IP Phones	Automatic phone provisioning on page 32 Manual phone provisioning on page 35	
8	Set up the Provisioning Server for the Manual provisioning.	Provisioning Server configuration on page 45	
9	Connect Avaya J100 Series IP Phones to the power supply and network with the Ethernet cable.	Power specifications on page 21	
10	Perform the phone initialization following the tasks for one of the selected methods.	Phone initialization on page 40	

Installing the wireless module

Before you begin

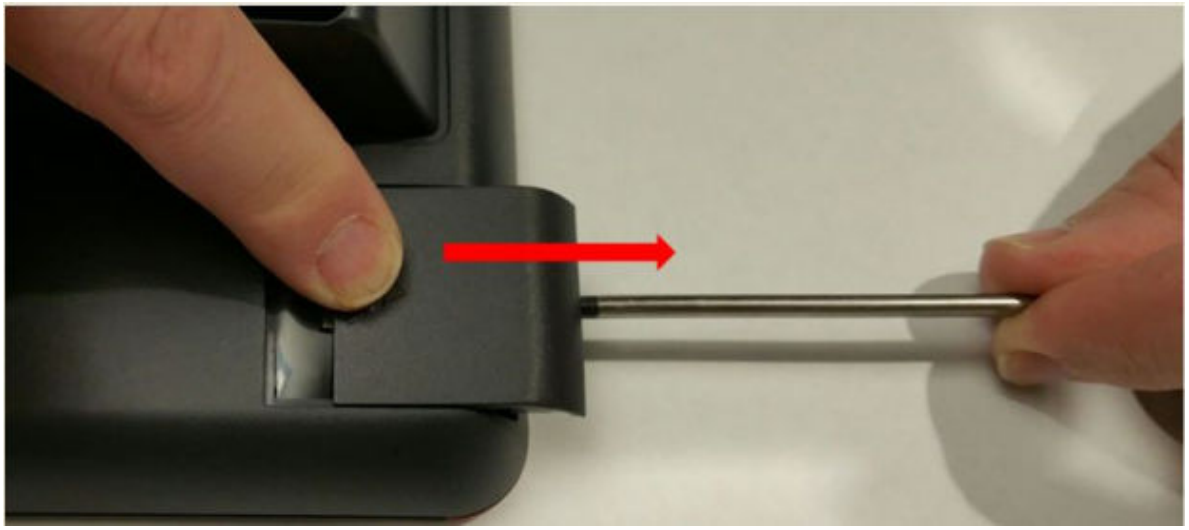
Obtain the following items:

- Phillips #1 screw driver to install the screw of the Avaya J100 Wireless Module.
- A flat screw driver that fits in the opening of the module panel.

Procedure

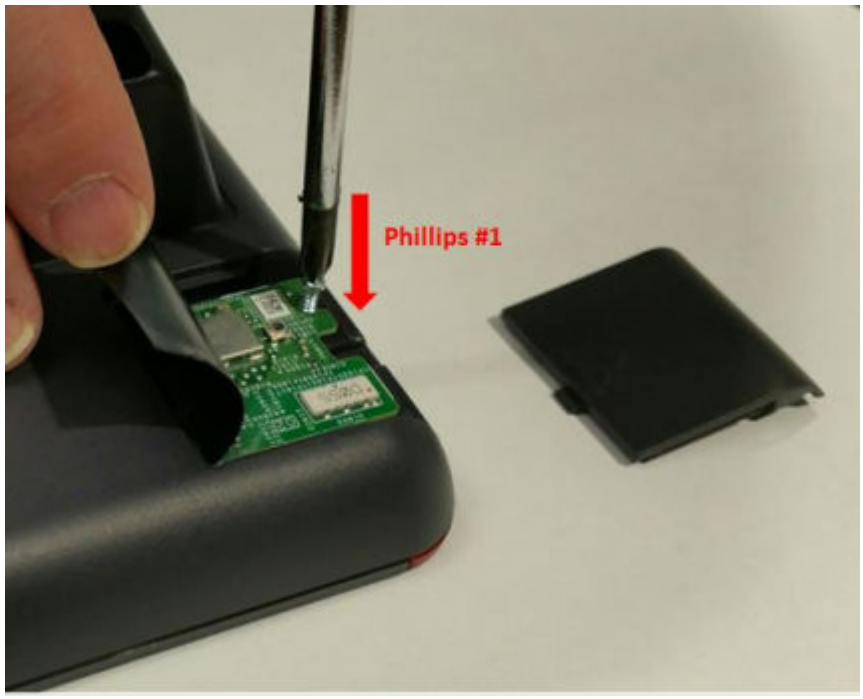
1. Insert the screw driver in the opening of the module panel to release the latch. Do not pry open the panel.

2. To remove the module panel, slide the panel out in the direction of the arrow.



3. Insert the Avaya J100 Wireless Module to the edge connector.

4. Use the Phillips #1 screwdriver to fasten the module.



5. Slide the module panel inward to close.

Wireless Module configuration

You can configure a Wi-Fi network by:

- Setting Wi-Fi parameters in the `46xxsettings.txt` file
- Configuring Wi-Fi parameters through the phone UI
- Configuring Wi-Fi parameters through the web UI

Note:

VLAN and LLDP functionalities are not supported over a wireless network.

Wall mounting Avaya J100 Series IP Phones

About this task

The wall mount kit is not bundled with the phone package. You must separately purchase the wall mount kit that is unique to your phone model. Use the following part numbers to order the wall mount kit:

- J129 phones — 700512707.
- J139, J159, J169, J179, and J189 phones — 700513631.

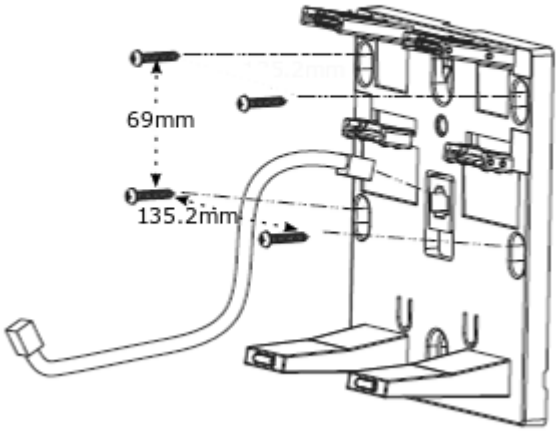
Before you begin

Obtain the following items:

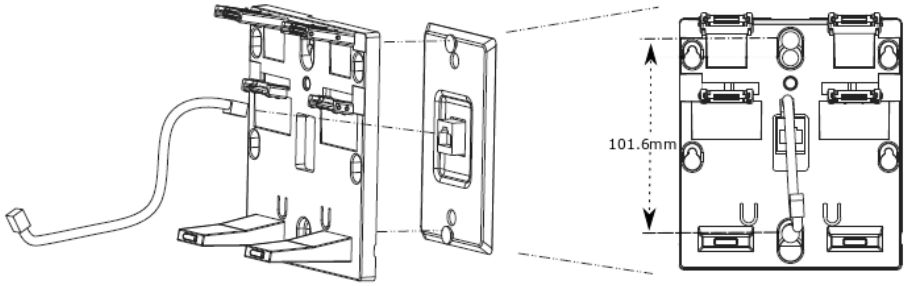
- Wall mounting kit, containing a wall mount bracket, and an Ethernet cable.
- Four #8 screws. The screws are not provided with the wall mounting kit. If the wall plate is pre-installed, you do not need the screws.

Procedure

1. Do one of the following:
   - Place the bracket on the wall and mark to drill holes. Use four #8 screws to fix the bracket.

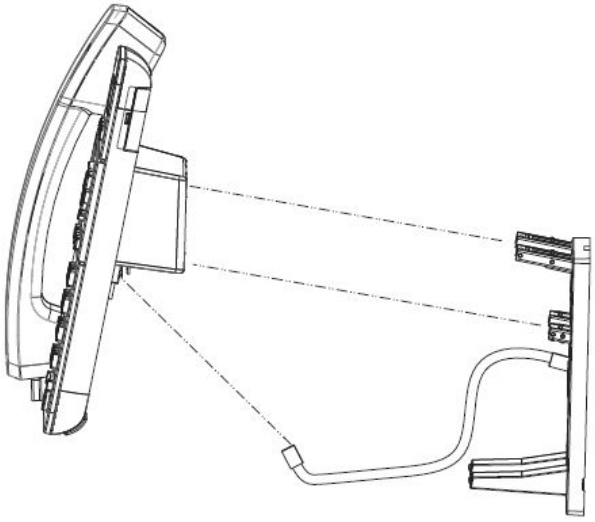


- If the wall plate is pre-installed, fit the wall mount bracket over the wall plate.



2. Connect one end of the Ethernet cable to the network port of the phone and the other end to the wall jack.
3. To attach the phone to the wall mount bracket, insert the two upper tabs of the bracket into the slots on the back panel of the phone.

   The lower pair of tabs rest against the back panel. The phone does not move when you press a key on the phone.



Wall mounting Avaya J100 Expansion Module

About this task

If your phone is wall mounted, you must additionally install the wall mount for the Avaya J100 Expansion Module. You must separately purchase the wall mount for the expansion module. The part number of the wall mount kit is 700514338.

Before you begin

Obtain the following items:

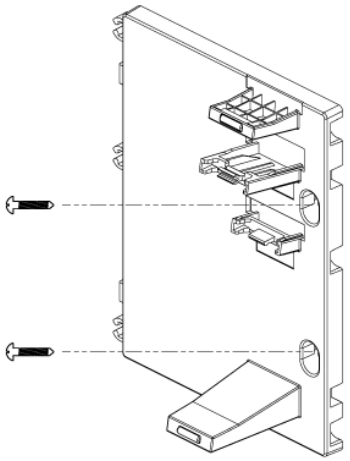
- Wall mount kit, containing a wall mount bracket.
- Two #8 screws. The screws are not provided with the wall mounting kit.
- Link for connecting expansion module for Avaya J189 IP Phone that comes along with the kit.

Procedure

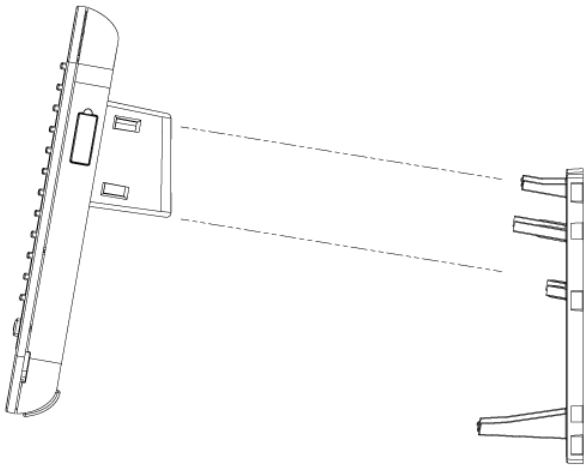
1. Remove the phone from the wall mount.
2. Place the expansion module bracket on one level to the right of the phone bracket, mark and drill holes, and then affix the #8 screws.

   Note:

   Use the link for installing wall mounting kit of Avaya J189 IP Phone.



3. To attach the Avaya J100 Expansion Module to the wall mount bracket, insert the upper tab of the bracket into the slot on the back panel of the expansion module.



4. Connect the expansion module to the phone as one assembled unit.
5. Connect the ethernet to the assembled unit.
6. Attach the phone to the wall mount bracket.

Software installation

You can install Avaya J100 Series IP Phones in the following ways:

- Automatically, using the Device Enrollment Services. Device Enrollment Services redirects the phone to the provisioning server and the phone initialization begins automatically.
- Manually, by performing the following configuration tasks:
  - Configuring the provisioning server
  - Supplying the provisioning server address to the phone by choosing one of the phone configuration methods

For best practices of phone installation, see Phone installation - best practices on page 376.

Identifying the device type during phone boot-up

About this task

Avaya J100 Series IP Phones screen displays the device type during phone boot-up to make the appropriate configuration for your device type. This feature is supported from the phone software version 4.0.3 and later.

Procedure

1. Set up the phone hardware.
2. Plug the Ethernet cable to the phone.

   The phone powers up and starts to initialize.

   The Open SIP phones display Open SIP text for all the J100 models except Avaya J129 IP Phone. Avaya J129 IP Phones display `Starting... Open SIP`.

Automatic phone provisioning

Device Enrollment Services server

Device Enrollment Services is an Avaya cloud service used to automate the deployment of phones, especially during initial deployment. Installing the phone by using Device Enrollment Services eliminates the need for manual configuration of a provisioning server. Device Enrollment Services is available at `des.avaya.com`.

Device Enrollment Services phone interface

The phone which supports Device Enrollment Services comes from the factory with a unique device certificate that is known to the Device Enrollment Services server. The phone's firmware includes a list of trusted root certificates of well-known public certificate authorities. The phone is programmed with the identity of the Device Enrollment Services services, `des.avaya.com`.

Related links

Automatic phone provisioning using Device Enrollment Services on page 33
Provisioning server mutual authentication support on page 34

Automatic phone provisioning using Device Enrollment Services

During initial boot-up, the phone prompts users to select if they want to contact the Device Enrollment Services server. The phone displays the `Do you want to activate Auto Provisioning now` prompt.

The user has 60 seconds to select **Yes** or **No** options, or the timeout is activated.

The following options are available:

- **Yes**: This option indicates that the phone should use only Device Enrollment Services for server discovery instead of a local network.

  If the phone can contact Device Enrollment Services and can obtain the configuration server URL, it contacts the configuration server to get the settings. If the phone fails to contact the configuration server, it prompts the user to enter the configuration server information manually.

  If the phone can contact Device Enrollment Services, but there is no configuration server assigned to the phone on Device Enrollment Services, it prompts the user to enter the numeric enrollment code.

  The numeric enrollment code is an 8 digit or 12 digit number as defined in Device Enrollment Services. For more information, see Device Enrollment Services administration documents at http://support.avaya.com/.

  When the user enters the numeric enrollment code, the phone contacts Device Enrollment Services again to obtain data on its configuration server and contacts the configuration server to download the settings.

  The user can cancel the operation of entering the numeric enrollment code. In this case, they are prompted to enter the configuration server manually.

- **No**: This option indicates that the phone should not use Device Enrollment Services and should discover the configuration server using the existing mechanism based on DHCP SSON, LLDP, PnP or Administration menu. If the phone fails to discover the configuration server using DHCP SSON, LLDP or PnP it prompts the user to enter the provisioning details manually.
- **Timeout**: After 60 seconds, if no option is selected, the phone uses the existing mechanism based on DHCP SSON, LLDP or PnP. If the phone fails to discover the configuration server, in this case, it contacts Device Enrollment Services to get the configuration server URL.

Related links

Automatic phone provisioning on page 32

Entering the provisioning details

About this task

You can enter the provisioning server address on the phones when the phone displays the Enter provisioning details screen.

Before you begin

Obtain the provisioning server address from the system administrator.

Procedure

1. If the phone does not receive the provisioning server address from the Device Enrollment Services or the DHCP SSON, LLDP or PnP, the phone displays the Enter provisioning details screen.
2. On Enter provisioning details screen, press one of the following:
   - **Config**: To enter the provisioning server address.
   - **Never**: To never prompt for the provisioning server address.
   - **Cancel**: To cancel the prompt and display the Login screen.
3. After you press **Config**, enter the provisioning server address in the **Address** field.

   The address is an alphanumeric URL. For example, `http://myfileserver.com/j100/`.

   Tip:

   To enter the dot symbol (.) in the field, press the alphanumeric soft key to toggle to the ABC mode.

   To enter the forward-slash symbol (/) in the field, press the / soft key.
4. **(Optional)** Enter the **Group** number.

   The value ranges from 0 to 999. If you do not enter a value, the phone uses the default value of 0.
5. Press **Save**.

   The phone continues the boot process and connects to the provisioning server.

Related links

Setting Up the Avaya J179 IP Phone (video)

Provisioning server mutual authentication support

Use the Device Enrollment Services server to install a client identity certificate on the phone. The phone uses the identity certificate for EAP TLS and mutual TLS authentication.

During mutual TLS authentication, the phone validates the certificate provided by the provisioning server and presents an identity certificate to the provisioning server. To validate the certificate, the provisioning server must trust the root CA certificate used for issuing the phone identity certificate.

You can configure the Device Enrollment Services server so that the phone needs an identity certificate for mutual authentication with the provisioning server. The phone requests for the certificate and then queries the Device Enrollment Services server for the provisioning server URL.

To use this functionality, you must install the Avaya Devices root certificate for issuing identity certificates on the provisioning server.

For more information on installing Device Enrollment Services HSM root certificate, see Avaya Device Enrollment Services documentation.

Related links

Automatic phone provisioning on page 32
Disabling DES on page 35

Disabling DES

During the first boot-up, you can disable the Device Enrollment Services discovery in one of the following ways:

- by setting the DES_STAT parameter to 0 or 1 in DHCP option 242
- by setting the DES_STAT parameter to 0 or 1 in the `46xxsettings.txt` file
- by disabling **DES Discovery** in the phone web interface (**Management** > **Device Enrollment Service** > **DES Discovery**)

Related links

Provisioning server mutual authentication support on page 34

Manual phone provisioning

This section describes the procedure to install the phone without invoking the Device Enrollment Services discovery process.

Related links

Prerequisites on page 35
Phone administration methods on page 36
Installation checklist on page 39

Prerequisites

Check the prerequisites to ensure that you have the required software and hardware before you install the Avaya J100 Series IP Phones.

Software requirements

Ensure that your network has the following components installed and configured:

- A DHCP server for providing dynamic IP addresses to the Avaya J100 Series IP Phones.
- A provisioning server, an HTTP or an HTTPS for downloading the software distribution package and the settings file.

For more information about installing and configuring the components, see their respective documentation.

Hardware requirements

Ensure that the LAN uses:

- Ethernet Category 5e or Ethernet Category 6 cabling.
- Either the 802.3at PoE or the 802.3af PoE injector specification.

Related links

Manual phone provisioning on page 35

Phone administration methods

You can use the following methods to administer the phone:

- DHCP
- LLDP
- Administration menu on the phone
- Web interface of the phone
- `46xxsettings.txt` file
- Prompt on the phone for entering the provisioning details on the first time boot-up

The following table lists the group of configuration parameters that you can administer through each of the corresponding methods:

Method	Can administer							
	IP addresses	Tagging and VLAN	Provisioning Server	Group	Network Time Server	Domain Name Server	Quality of Service	Application-specific parameters
DHCP	✔	✔	✔	—	✔	✔	✔	✔
LLDP	—	✔	✔	—	—	—	✔	—

Table continues…

Method	Can administer							
Administration menu on the phone	✔	✔	✔	✔	✔	✔	—	✔
Web interface of the phone	✔	✔	✔	✔	✔	✔	✔	✔
`46xxsettings.txt` file	—	✔	✔	—	✔	✔	✔	✔
Phone prompts for provisioning details on the first time boot-up	—	—	✔	✔	—	—	—	—

Precedence of the administration methods

You can configure most of the parameters using multiple configuration methods. If you configure a parameter through more than one method, the device applies the settings of the highest precedence method. The following list shows the precedence of the methods in the order from highest to lowest:

1. Administration menu on the phone
2. Web UI

   The web interface of the phone has the same precedence as the Administration menu
3. Settings file
4. DHCP
5. LLDP.

   Network Layer 2 related parameters such as L2QVLAN, L2Q, L2QAUD, L2QSIG, DSCPAUD, DSCPSIG, and PHY2VLAN configured using LLDP, have higher precedence over other sources if the same settings are provided through other administrative methods.

Related links

Manual phone provisioning on page 35

Downloading and saving the software

Before you begin

Ensure that your provisioning server is set up.

Procedure

1. Go to the Avaya support website.
2. In the **Enter Your Product Here** field, enter Avaya J100 Series IP Phones.
3. In the **Choose Release** field, click the required release number.
4. Click the **Downloads** tab.

   The system displays a list of the latest downloads.
5. Click the appropriate software version.

   The system displays the Downloads page.
6. In the **File** field, click the zipped file and save the file on the provisioning server.
7. Extract the zipped file and save it at an appropriate location on the provisioning server.
8. From the latest downloads list, click the `Settings` file.

   The system displays the Downloads page.
9. In the **File** field, click the `Settings` file and save the file at an appropriate location on the provisioning server.

Software distribution package

Software distribution package contains the files needed to operate the Avaya J100 Series IP Phones packaged together in a ZIP format. You can download the package from the Avaya support website.

SIP software distribution package contains:

- Phone application file. For example, `FW_S_J129_R4_0_1.bin`
- Upgrade file, `J100Supgrade.txt`
- The MIB file
- Language files. For example, `Mlf_J129_BrazilianPortuguese.xml`, `Mlf_J129_Chinese.xml`
- Phone release file, `release.xml`

  The phone release file is used by the Avaya Software Update Manager application to maintain the firmware for Avaya-managed devices.

Important:

Ensure that you download the latest software distribution package and read any Product Support Notices (PSNs) associated with the new release available on the Avaya support website.

Review the release notes, and any Read Me files associated with a distribution package.

Ensure that the Settings file is not cached in your browser. You can clear the browser cache before downloading the settings file from the Avaya support website to not get an old version.

Note:

To configure Open SIP root certificates, you can use the TRUSTCERTS parameter in the `46xxsettings.txt` file. The supported file format is `.pem`.

Modifying the settings file

About this task

Use this procedure to modify the `46xxsettings.txt` file to provision the phone configuration parameters. The parameter values stored for the users of a particular phone model do not apply to other phone models, even if the corresponding SIP user is the same.

Procedure

1. On the file server, go to the directory of the `46xxsettings.txt` file.
2. Open the `46xxsettings.txt` file in a text editor.
3. Set the values of the parameters that you want to provision.
4. Save the `46xxsettings.txt` file.

Result

On the next poll, the phones download the `46xxsettings.txt` file and apply the configuration settings.

Installation checklist

Use this checklist to gather, record, and follow the procedure for the installation.

No.	Task	Reference	✔
1	Check the prerequisites.	Prerequisites on page 35	
2	Administer VLAN.	VLAN overview on page 61	
3	Configure the servers.	Provisioning server configuration on page 45	
4	Download and save the software package.	Downloading and saving the software on page 37	
5	Configure the Settings file.	Configuration parameters on page 387	
6	Configure the Upgrade file.	Device upgrade process on page 376	
7	Install the phone.	Phone initialization on page 40	

Related links

Manual phone provisioning on page 35

Phone initialization

Before you begin

You must do the following:

- Configure the provisioning server.
- Download and extract the firmware zip file to your provisioning server.
- Configure the `46xxsettings.txt` file.

Procedure

1. Set up the phone hardware.
2. Plug the Ethernet cable to the phone.

   The phone powers up and starts to initialize.
3. The initialization procedure consists of the following processes:
   a. The phone prompts the user to activate auto provisioning.
   b. The phone checks for LLDP messages.
   c. The phone sends a DHCP DISCOVER message to discover the DHCP server in the network and invokes the DHCP process.

      If the phone does not receive a provisioning server address from the configuration setup, the phone displays the Enter provisioning details screen.
   d. In the Enter provisioning details screen, press the **Config** soft key and enter the address of the provisioning server. The address is an alphanumeric URL like http://myfileserver.com/j100/. To enter the dot symbol (.) in the field, press the alphanumeric soft key to toggle to the alphanumeric mode.
   e. The phone verifies the VLAN ID, and starts tagging the data and voice packets accordingly.
   f. The phone queries the HTTP server directory defined by HTTPDIR, to find the `J100Supgrade.txt` and the `46xxsettings.txt` file. If the files cannot be found, the phone reverts to looking into the root directory of the HTTP server.
   g. The phone gets the `J100Supgrade.txt` file, the `46xxsettings.txt` file, the language files, and any firmware updates.
      - If configured to use simple certificate enrollment protocol (SCEP), the phone downloads a valid device certificate.
      - The phone displays only the **Admin** soft key for 15 seconds, and then the **Admin** and the **Login** soft keys.

        Note:

        For subsequent restarts, if the user login is automatic and the supplied credentials are valid, the **Login** soft key is not displayed.

4. Do one of the following:
   - To access the user login screen, press the **Login** soft key.
   - To access the Admin menu, press the **Admin** soft key and enter the admin menu password.

   To ensure that the phone is properly installed and running properly, verify using the Post installation checklist.

Related links

Post installation checklist on page 382

Cloud configuration

Configuration through a cloud server

Cloud server configuration simplifies the process of deployment and is applicable when the phone must be configured on an Open SIP server. The cloud vendor assigns a customer reference number and creates a sub-directory on its file server. The cloud vendor must generate the following for creating a customer profile:

- Customer username
- Customer password
- Customer extension number

The cloud vendor must have a staging area file server to host the customer-specific settings. Customer-specific settings are generated for each customer through the MAC address of the phone. A file where the filename is the MAC address of the phone must be hosted on the staging area file server.

The staging area file server must host the following files:

- `J100Supgrade.txt`
- `46xxsettings.txt`

  Note that `46xxsettings.txt` file must contain command "GET $MACADDR.txt"
- `$MACADDR.txt`
- Software upgrade files available from Avaya

Phone setup process on a cloud server

The phone does the following during the setup process:

1. Boots and discovers the staging area file server address through DHCP.

2. Retrieves and checks the `J100Supgrade.txt` file for device upgrade if required.
3. Retrieves the `46xxsettings.txt`.
4. The line GET $MACADDR.txt is parsed by the J100 device. It replaces $MACADDR with the devices actual MAC Address. For example: aabbccddeeff
5. Retrieves aabbccddeeff.txt file for customer-specific configurations.
6. Logs on to the SIP Proxy server of the cloud service provider.

Settings file contents on a cloud server

The cloud server hosts the common configuration for all Avaya J100 Series IP Phones through the `46xxsettings.txt` file. The `46xxsettings.txt` file must contain a line entry for the device to obtain a separate configuration file unique to the device.

Settings file contents

SET ENABLE_3PCC_ENVIRONMENT 1

SET 3PCC_SERVER_MODE 0

SET $MACADDR.txt

where, `MACADDR.txt` is the MAC address of the phone. `MACADDR.txt` must be in lower- case, for example

```
GET $MACADDR.txt c81fec823ec4.txt
```

MAC address file contents on a cloud server

The cloud server hosts a MAC address file that contains customer details. This file is unique to each phone and can also be used for custom settings for a specific phone. Note that the parameters defined in `$MACADDR.txt` file have precedence over the same parameters defined in `46xxsettings.txt` file.

MAC address file contents

```
SET <HTTPSRVR> <"">
SET <TLSDIR> <"">
SET <FORCE_SIP_EXTENSION> <"">
SET <FORCE_SIP_PASSWORD> <"">
SET <FORCE_SIP_USERNAME> <"">
```

where,

- HTTPSRVR with `<"″>` is the name of the parameter that removes the cached HTTP file server address. This redirects the phone to the cloud service provider's file server.
- TLSDIR is the name of the parameter that locates the sub-directory of the cloud service provider.
- FORCE_SIP_EXTENSION is the name of the parameter that assigns the auth id or user name.
- FORCE_SIP_PASSWORD is the name of the parameter that assigns the password.

- FORCE_SIP_USERNAME is the name of the parameter that assigns the user id or phone number or extension.

Chapter 4: Servers, VLAN, and IP configuration

Server configuration

To install Avaya J100 Series IP Phones in your telephony environment, you must configure the following servers:

- DHCP server: To dynamically assign IP addresses to the devices and optionally provide the other configuration parameters to the device. The DHCP server also provides the device with the addresses of the SIP controller and the provisioning server.
- HTTP or HTTPS provisioning server: To download and save the software distribution package and the settings file. To provide software distribution package (J100Supgrade.txt), configuration files (46xxsettings.txt) and resource files such as custom ringtones, backgrounds, screensavers, and certificates.
- SNTP server: To provide the device with accurate date and time.
- DNS server: To allow the device to resolve URL/FQDN addresses to IP addresses.
- STUN server: To allow the device to discover its public IP address and ports for SIP signaling.

Related links

Configuration through DHCP on page 50

Setting up a provisioning server

About this task

Use this procedure to configure an HTTP or HTTPS file server. You can use the provisioning server to download and store distribution packages and settings files for the phones.

Procedure

1. Install the HTTP or HTTPS server software according to the software vendor’s instructions.

   For the Avaya J100 Series IP Phones to connect to an HTTPS server the device must trust the HTTPS server. The phone must have the HTTPS server's root CA available to validate the HTTPS Server. By default the Avaya J100 Series IP Phones support many well known public CA certificates. See, ENABLE_PUBLIC_CA_CERTS in the Appendix section.

Alternatively, if your provisioning server does not support use of a well known public CA the Avaya J100 Series IP Phones can be configured to obtain additional certificates. See, TRUSTCERTS in the Appendix section.

2. Download the software distribution package and the `46xxsettings.txt` settings file.
3. Extract the distribution package, and save the extracted files and the `46xxsettings.txt` settings file on the provisioning server.

Provisioning Server configuration

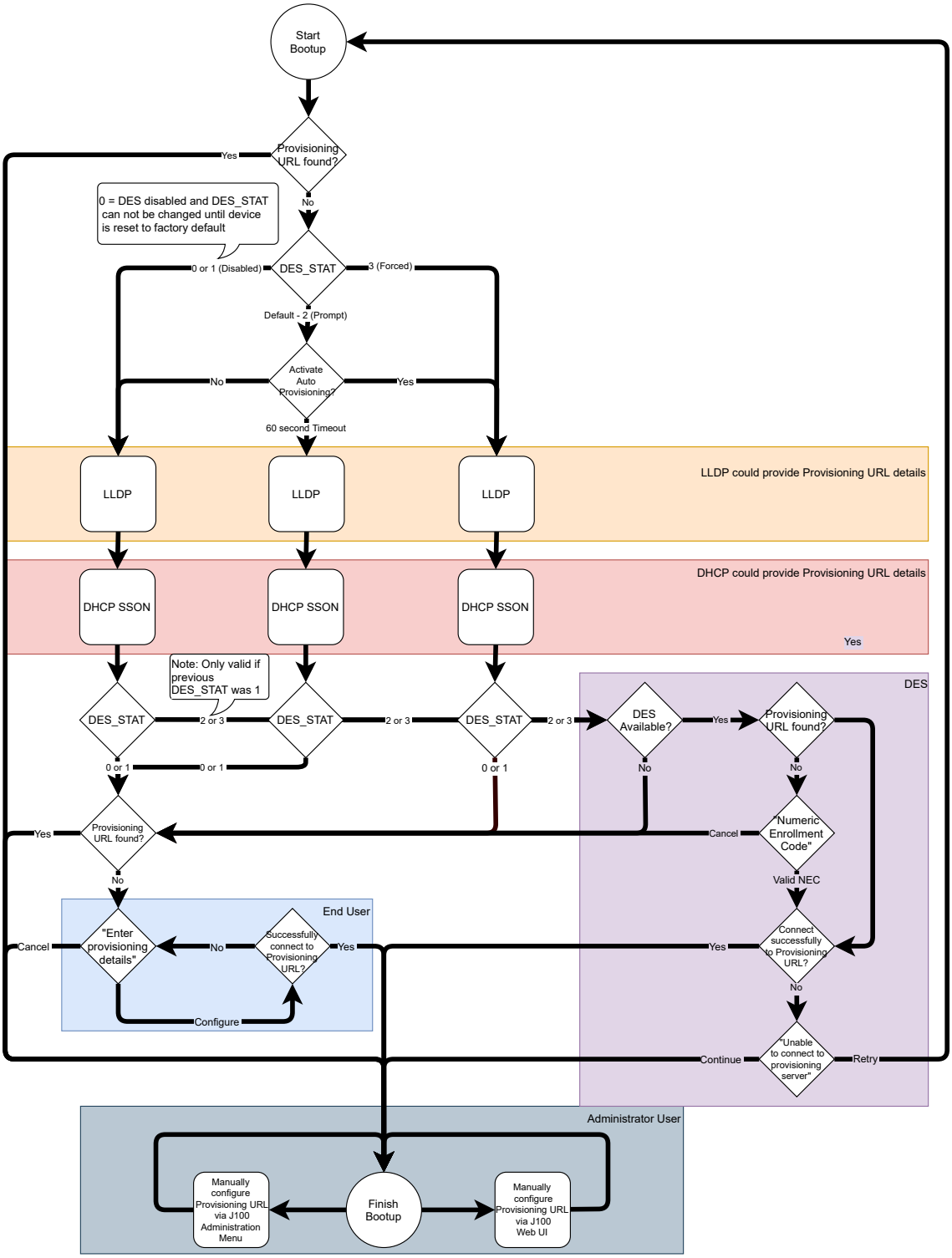
A provisioning server is an HTTP or an HTTPS server that the Avaya J100 Series IP Phones connect to obtain the phone software files and configuration settings files.

When the Avaya J100 Series IP Phones boot up, or is performing a check for updates, the phone checks for firmware updates and configuration files on the configured provisioning server.

The following methods are available to configure the Avaya J100 Series IP Phones provisioning server address:

- DHCP
- LLDP
- Device Enrollment Services (DES)
- Administration menu on the phone
- Web interface of the phone
- Prompt on the phone for entering the provisioning details on the first time boot-up

The following flow chart depicts how Avaya J100 Series IP Phones can obtain the Provisioning server address:


Start Bootup
Provisioning URL found?
Yes
No
0 = DES disabled and DES_STAT can not be changed until device is reset to factory default
DES_STAT
0 or 1 (Disabled)
3 (Forced)
Default - 2 (Prompt)
Activate Auto Provisioning?
No
Yes
60 second Timeout
LLDP
LLDP
LLDP
LLDP could provide Provisioning URL details
DHCP SSON
DHCP SSON
DHCP SSON
DHCP could provide Provisioning URL details
Yes
Note: Only valid if previous DES_STAT was 1
DES_STAT
2 or 3
DES_STAT
2 or 3
DES_STAT
2 or 3
0 or 1
0 or 1
0 or 1
DES
DES Available?
Yes
No
Provisioning URL found?
Yes
No
Provisioning URL found?
Yes
No
Cancel
"Numeric Enrollment Code"
Valid NEC
End User
"Enter provisioning details"
Cancel
No
Successfully connect to Provisioning URL?
Yes
Configure
Connect successfully to Provisioning URL?
Yes
No
"Unable to connect to provisioning server"
Continue
Retry
Administrator User
Manually configure Provisioning URL via J100 Administration Menu
Finish Bootup
Manually configure Provisioning URL via J100 Web UI

SNTP server configuration

Simple Network Time Protocol (SNTP) is a mechanism that the devices use for time-synchronization. This is possible because of the network time server that runs on the devices.

SNTP specifies the IP address or DNS of the network time server. You can configure SNTP using one of the following methods listed in the table:

No	Method	Notes
1	DHCP option 42	You can configure DHCP option 42 that provides SNTP IP address list. See DHCP options in Related links.
2	`46xxsettings.txt` file	Use the settings file for configuring date and time using SNTP parameter. See SNTP parameter in Related links.
3	Administration menu on the phone	Use the administration menu to update the SNTP server information on the phone. See IP configuration field description in Related links.
4	Web interface of the phone	Use the **IP Configuration** field for updating SNTP server information using the web interface of the phone. See Ethernet settings field descriptions in Related links.

On Avaya J100 Series IP Phones, the value of SNTPSRVR parameter can be a comma-separated list of SNTP server addresses, which can be IPv4 or IPv6 addresses. This parameter has following values:

0.avaya.pool.ntp.org,1.avaya.pool.ntp.org,2.avaya.pool.ntp.org, 3.avaya.pool.ntp.org

If these servers are not reachable, you can configure the phone with an alternate list of SNTP servers. Set the SNTPSRVR parameter value in the `46xxsettings.txt` file to ntpserver-1,ntpserver-1,ntp-server-2. It provides IP address or FQDN of the desired NTP server(s). Specifying the correct SNTPSRVR prevents the delay caused by the phone waiting for NTP server timeouts.

Related links

SNTP Parameters on page 47
DHCP options on page 51
IP configuration field description on page 95
Ethernet settings field descriptions on page 133

SNTP Parameters

Use the `46xxsettings.txt` settings file for configuring date and time using the following parameters.

Parameter name	Default Value	Description
SNTPSRVR	Null	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.
SNTP_SYNC_INTERVAL	1440 minutes	Specifies the time interval, in minutes, during which the phone attempts to synchronize its time with configured NTP servers. Valid values are from 60 to 2880 minutes.
GMTOFFSET	0:00	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 to 59 (minutes).
DSTOFFSET	1	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.
DSTSTART	2SunMar2L	Specifies when to apply the offset for daylight savings time. The date and time for applying the offset can be set in the following formats: • `odddmmmht`: for example, `2SunMar2L` which corresponds to the second Sunday in March at 2 AM local time; • `Dmmmht`: for example, `10Mar5L` which corresponds to March 10 at 5 AM local time.

Table continues…

Parameter name	Default Value	Description
DSTSTOP	1SunNov2L	Specifies when to stop applying the offset for daylight savings time. You can set the date and time when the offset is stopped in the following formats: • `odddmmmht`: for example, `1SunNov2L` which corresponds to the first Sunday in November at 2 AM local time; • `Dmmmht`: for example, `7Nov5L` which corresponds to November 7 at 5 AM local time.

Related links

SNTP server configuration on page 47

DHCP server configuration

You can configure the DHCP server to:

- Dynamically assign IP addresses to Avaya J100 Series IP Phones.
- Provision phone and site-specific configuration parameters through various DHCP options.

In a Device Enrollment Services (DES) environment, the DHCP server is primarily used to assign IP addresses to the phones. The phones receive the provisioning server address from the DES server.

Related links

Setting up a DHCP server on page 49

Setting up a DHCP server

About this task

Use this procedure to set up a third-party DHCP server.

Before you begin

Contact your server software vendor to obtain server software installation and configuration instructions.

Procedure

1. Install the DHCP server software according to the software vendor’s instructions.
2. Create a DHCP scope to define the range of IP addresses for the phones.

3. Configure the required DHCP options.

   The DHCP site-specific option that you configure must match the Site Specific Option Number (SSON) that the phones use. The default SSON that the phones use is 242.

Related links

DHCP server configuration on page 49

Configuration through DHCP

Avaya J100 Series IP Phones connect to the DHCP server during the boot up. You can configure the DHCP server to provide the following information to the device:

- IP address
- Subnet mask
- IP address of the router
- IP address of the SNTP server
- IP address of DNS

You can configure the DHCP server to:

- Dynamically assign IP addresses to the Avaya J100 Series IP Phones.
- Provide various configuration parameters to the Avaya J100 Series IP Phones by configuring Option 43 Vendor-specific options or SSON (site-specific option) in the DHCP server.

Setting up a DHCP server

About this task

Use this procedure to set up a third-party DHCP server.

Before you begin

Contact your server software vendor to obtain server software installation and configuration instructions.

Procedure

1. Install the DHCP server software according to the software vendor’s instructions.
2. Create a DHCP scope to define the range of IP addresses for the phones.
3. Configure the required DHCP options.

   The DHCP site-specific option that you configure must match the Site Specific Option Number (SSON) that the phones use. The default SSON that the phones use is 242.

Related links

DHCP server configuration on page 49

DHCP options

You can configure the following options in the DHCP server:

Option	Description
Option 1	Specifies the subnet mask of the network.
Option 3	Specifies the gateway IP address list. The list can contain up to 127 total ASCII characters. Separate more than one IP address with commas with no intervening spaces.
Option 6	Specifies the DNS server address list. The list can contain up to 127 total ASCII characters. Separate more than one IP address with commas with no intervening spaces. The phone supports DNS and the dotted decimal addresses. The phone attempts to resolve a non-ASCII-encoded dotted decimal IP address by checking the contents of DHCP Option 6. At least one address in Option 6 must be a valid, nonzero, dotted decimal address, otherwise the DNS address fails.
Option 12	Avaya J100 Series IP Phones identify themselves to the DHCP server by sending the host name in Sub-Option 12 in `DHCP DISCOVER` and `DHCP REQUEST` options. The host name has the following format: `AVohhhhhh`, where: • `AV` stands for Avaya. • `o` is one of the following values based on Object Unique Identifier (OUI) derived from the first three octets of the phone MAC address: - A if OUI is 00-04-0D - B if OUI is 00-1B-4F - E if OUI is 00-09-6E - L if OUI is 00-60-1D - T if the OUI is 00-07-3B - X if the OUI is anything else • `hhhhhh` are the ASCII characters for the hexadecimal representation of the last three octets of the phone MAC address.

Table continues…

Option	Description
Option 15	Specifies the domain name. The domain name is required to resolve DNS names into IP addresses. Configure this option if you use a DNS name for the HTTP server. Otherwise, you can specify a domain as part of customizing the HTTP server. This domain name is appended to the DNS addresses specified in Option 6 before the phone attempts to resolve the DNS address. The phone queries the DNS address in the order they are specified in Option 6. If there is no response from an address, the phone queries the next DNS address. As an alternative to administering DNS by DHCP, you can specify the DNS server and domain name in the HTTP script file. If you use the script file, you must configure the DNSSRVR and DOMAIN parameters so that you can use the values of these parameters in the script. Administer Option 6 and Option 15 appropriately with DNS servers and domain names respectively.
Option 42	Specifies the SNTP IP address list. List servers in the order of preference. The minimum length is 4 and the length must be a multiple of 4.
Option 43	Specifies the encapsulated vendor-specific options that clients and servers use to exchange the vendor-specific information. Option 43 is processed only if the first code in the Option is 1 with a value of 6889. The value 6889 is an Avaya enterprise number. All values are interpreted as strings of ASCII characters that are accepted with or without a null termination character. Any invalid value is ignored and the corresponding parameter value is not set. Cannot be used simultaneously with DHCP SSON (Option 242).
Option 51	Specifies the DHCP lease time. If this option is not received, the DHCPOFFER is not accepted. Assign a lease time of six weeks or greater. If this option has a value of FFFFFFFF hex, the IP address lease is assumed to be infinite, so that the renewal and rebinding procedures are not necessary even if Options 58 and 59 are received. Expired leases causes the device to reboot.
Option 52	Specifies the overload option. If this option is received in a message, the device interprets the name and file parameters.
Option 53	Specifies the DHCP message type. The value can be one of the following: • 1 for DHCPDISCOVER • 3 for DHCPREQUEST For DHCPREQUEST sent to renew the device IP address lease: • If a DHCPACK is received in response, a log event record is generated with a Log Category of DHCP. • If a DHCPNAK is received in response, the device immediately ceases IP address usage, generates a log event record, sets IPADD to 0.0.0.0, and enters the DHCP INIT state.

Table continues…

Option	Description
Option 55	Specifies the parameter request list. Acceptable values are: • 1 for subnet mask • 3 for router IP addresses • 6 for domain name server IP addresses • 7 for log server • 15 for domain name • 42 for NTP servers
Option 57	Specifies the maximum DHCP message size. Set the value to 1500. Set the value to 1000.
Option 58	Specifies the DHCP lease renew time. If not received or if this value is greater than that for Option 51, the default value of T1, renewal timer is used.
Option 59	Specifies the DHCP lease rebind time. If not received or if this value is greater than that for Option 51, the default value of T2, rebinding timer is used.
Option 242	Specifies the site-specific option (SSON). It is optional but cannot be used simultaneously with Option 43. If you do not configure this option, ensure that one of the following parameters is configured appropriately elsewhere: • HTTPSRVR • TLSSRVR

Related links

SNTP server configuration on page 47
Signaling protocol on page 97

DHCP vendor-specific option

You can set DHCP vendor-specific parameters by using DHCP option 43. The supported codes for Option 43 and the corresponding parameters are as follows:

Code	Parameter
1	Does not set any parameter. The value must be 6889.
2	HTTPSRVR
3	HTTPDIR
4	HTTPPORT
5	TLSSRVR
6	TLSDIR
7	TLSPORT

Table continues…

Code	Parameter
8	TLSSRVRID
9	L2Q
10	L2QVLAN
11	PHY1STAT
12	PHY2STAT
14	SIG
15	SIP_CONTROLLER_LIST

Extending use of DHCP lease

Avaya J100 Series IP Phones support configuration of network parameters using DHCP as per RFC 2131. However, when a DHCP server becomes unreachable and the DHCP lease currently held by the phone expires, the phone continues to use the same lease until the DHCP server becomes reachable. This functionality is controlled by setting the following parameter:

Parameter name	Default value	Description
DHCPSTD	0	Specifies if the expired DHCP lease is used. Value operation: • 0: Continue use of the expired DHCP lease if the lease could not be renewed. • 1: Stop using the DHCP lease immediately when it expires, as per the standard. The parameter is configured through the `46xxsettings.txt` file.

When this feature is enabled (DHCPSTD=1), the phone continues to use the lease data, including IP address, router and other options if the lease could not be renewed. In this state, the phone will attempt to reach a DHCP server every 60 seconds. When a DHCP server becomes available and a lease is renewed or new lease obtained, the phone performs a duplicate address detection on the offered IP address. If no conflicts are detected, this IP address is assigned to the local network interface for use.

Parameter configuration through DHCP

Avaya J100 Series IP Phones support the DHCP configuration option called Site Specific Option (SSON). Using this option, custom parameters can be configured on the phone through a DHCP server. In DHCP DISCOVER, the phone requests for the SSON, typically configured in DHCP Option 242. To respond to this request, configure the DHCP server with proper data supplied in the offer for this option value. The following is an example of such configuration:

```
option avaya-option-242 L2Q=1,L2QVLAN=1212,httpsrvr=192.168.0.100
```

The following parameters can be configured with this feature:

Parameter	Set to
DHCP lease time	Option 51, if received
DHCP lease renew time	Option 58, if received
DHCP lease rebind time	Option 59, if received
DOMAIN	Option 15, if received
DNSSRVR	Option 6, if received, which can be a list of IP addresses
HTTPSRVR	The siaddr parameter, if that parameter is non-zero
IPADD	The yiaddr parameter
LOGSRVR	Option 7, if received
MTU_SIZE	Option 26
NETMASK	Option 1, if received
ROUTER	Option 3, if received, which might be a list of IP addresses
SNTPSRVR	Option 42

DHCP site-specific option

You can set the values of site-specific configuration parameters through a DHCP option. The default DHCP option to set the site-specific configuration parameters is 242. You can also use any option between 128 to 254. Whichever option you select , you must specify that number in the Site-Specific Option Number (SSON) parameter by using the device interface.

The following is an example of the DHCP 242 option string that specifies the HTTPSRVR and the Voice VLAN that the device must connect to.

```
HTTPSRVR=10.138.251.67,L2QVLAN=1104
```

The following table lists the site-specific configuration parameters that you can define for the device:

Parameter	Description
ADMIN_PASSWORD	Specifies the security string used to access local procedures. The string can contain alphanumeric characters. The default is 27238. This parameter replaces PROCPSWD as it provides a more secure password syntax.
DSTOFFSET	Specifies the time offset in hours of daylight savings time from local standard time. The default value is 1.
DSTSTART	Specifies when to apply the offset for daylight savings time. The default value is 2SunMar2L, meaning the second Sunday in March at 2AM local time.
DSTSTOP	Specifies when to stop applying the offset for daylight savings time. The default value is 1SunNov2L, meaning the first Sunday in November at 2AM local time.

Table continues…

Parameter	Description
GMTOFFSET	Specifies the time offset from GMT in hours and minutes. The format begins with an optional plus (+) or minus (-). If you do not set any value, + is used. Followed by 0 through 12 hours, followed by a colon (:), followed by 00 through 59 minutes. The default value is 0:00.
HTTPDIR	Specifies the path to the configurations and data files in HTTP and HTTPS GET operations during device bootup. This path is relative to the root of the HTTPS file server, to the directory in which the device configuration and date files are stored. If $MACADDR and/or $MODEL4 and/or $SERIALNO macro is present in the configured path then such macro is replaced with its actual value.The path might contain maximum 127 characters without spaces. HTTPDIR is the path for all HTTP operations. The command is `HTTPDIR=<path>`. In configurations where the upgrade and binary files are in the default directory on the HTTP server, do not use `SET HTTPDIR=<path>`.
HTTPPORT	Specifies the destination port for HTTP requests. The default is 80.
HTTPSRVR	The firmware files are digitally signed, so TLS is not required for security.
ICMPDU	Controls the extent to which ICMP Destination Unreachable messages are sent in response to messages sent to closed ports so as not to reveal information to potential hackers. The default is 1, which sends Destination Unreachable messages for the closed ports used by traceroute.
ICMPRED	Controls whether ICMP Redirect messages are processed. The default is 0 in which redirect messages are not processed.
L2Q	Specifies the 802.1Q tagging mode. The default is 0 for automatic.
L2QVLAN	Specifies the VLAN ID of the voice VLAN. The default is 0.
PHY1STAT	Controls the Ethernet line interface speed. The default is 1 for auto-negotiate.
PHY2STAT	Controls the secondary Ethernet interface speed. The default is 1 for auto-negotiate.
PROCPSWD	Specifies the security string used to access local procedures. The value can be up to 7 ASCII numeric digits. The default is 27238.
PROCSTAT	Controls whether local procedures are enabled. The default is 0 for enabled.
REUSETIME	Specifies the time in seconds for IP address reuse. The default is 60 seconds.
SIP_CONTROLLER_LIST	Specifies the SIP proxy or registrar server IP or DNS addresses. The list contains 0 to 255 characters. The IP address must be in the dotted decimal name format, separated by commas and without intervening spaces. The default is null.
TLSDIR	Specifies the path to the configurations and data files in HTTPS GET operations during device bootup. This path is relative to the root of the HTTPS file server, to the directory in which the device configuration and data files are stored. If $MACADDR and/or $MODEL4 and/or $SERIALNO macro is present in the configured path then such macro is replaced with its actual value. The string can be from 0 to 127 characters long, without spaces.
TLSPORT	Specifies the destination TCP port used for requests to https servers in the range of 0 to 65535. The default is 443, which is the standard HTTPS port.

Table continues…

Parameter	Description
TLSSRVR	Specifies the IP address or DNS name of the file server that is used to download the configuration files. Firmware files can also be downloaded using HTTPS. **Note:** Transport Layer Security is used to authenticate the server.
VLANTEST	Specifies the number of seconds to wait for DHCPOFFER on a non-zero VLAN. The default is 60 seconds.

Configuration through LLDP

Link Layer Discovery Protocol (LLDP) is an open standards, layer 2 protocol that IP phones use to advertise their identity and capabilities and to receive administration from Ethernet switches. LAN equipment can use LLDP to manage power and administer VLANs, DSCP, and 802.1p priority fields.

The transmission and reception of LLDP is specified in IEEE 802.1AB-2005. The Avaya J100 Series IP Phones use Type-Length-Value (TLV) elements specified in IEEE 802.1AB-2005, TIA TR-41 Committee - Media Endpoint Discovery (LLDP-MED, ANSI/TIA-1057), and Proprietary elements. LLDP Data Units (LLDPDUs) are sent to the LLDP Multicast MAC address.

The Avaya J100 Series IP Phones running SIP software support IEEE 802.1AB if the value of the configuration parameter LLDP_ENABLED is “1” (On) or “2” (Auto). If the value of LLDP_ENABLED is “0” (off), the transmission and reception of Link Layer Discovery Protocol (LLDP) is not supported. When the value of LLDP_ENABLED is “2”, the transmission of LLDP frames does not begin until an LLDP frame is received. The first LLDP frame is transmitted within 2 seconds after the first LLDP frame is received. After transmission begins, an LLDPDU is transmitted every 30 seconds. A delay of up to 30 seconds in phone initialization might occur if the file server address is delivered by LLDP and not by DHCP.

These phones do not transmit 802.1AB multicast LLDP packets from an Ethernet line interface to the secondary line interface and vice versa.

By using LLDP, you can configure the following:

- Call server IP address
- File server
- PHY2VLAN
- L2QVLAN and L2Q
- DSCP
- 802.1p priority

LLDPDU transmitted by the phones

Category	TLV Name (Type)	TLV Info String (Value)
Basic Mandatory	Chassis ID	IPADD of phone, IANA Address Family Numbers enumeration value for IPv4, or subtype 5:Network address.
Basic Mandatory	Port ID	MAC address of the device.
Basic Mandatory	Time-To-Live	120 seconds.
Basic Optional	System Name	The Host Name sent to the DHCP server in DHCP option 12.
Basic Optional	System Capabilities	Bit 2 (Bridge) will be set in the System Capabilities if the phone has an internal Ethernet switch. If Bit 2 is set in Enabled Capabilities then the secondary port is enabled.
Basic Optional	Management Address	Mgmt IPv4 IP address of device. Interface number subtype = 3 (system port). Interface number = 1. OID = SNMP MIB-II sysObjectID of the device.
IEEE 802.3 Organization Specific	MAC / PHY Configuration / Status	Reports auto negotiation status and speed of the uplink port on the device.
TIA LLDP MED	LLDP-MED Capabilities	Media Endpoint Discovery capabilities = 00-33 (Inventory, Power-via-MDI, Network Policy, MED Caps).
TIA LLDP MED	Network Policy	Tagging Yes/No, VLAN ID for voice, L2 Priority, DSCP Value.
TIA LLDP MED	Inventory – Hardware Revision	MODEL - Full Model Name.
TIA LLDP MED	Inventory – Firmware Revision	Firmware version.
TIA LLDP MED	Inventory – Software Revision	Software version or filename.
TIA LLDP MED	Inventory – Serial Number	Device serial number.
TIA LLDP MED	Inventory – Manufacturer Name	Avaya.
TIA LLDP MED	Inventory – Model Name	MODEL with the final Dxxx characters removed.
Avaya Proprietary	Call Server IP address	Call Server IP Address. Subtype = 3.
Avaya Proprietary	IP Phone addresses	Phone IP address, Phone Address Mask, Gateway IP Address. Subtype = 4.
Avaya Proprietary	File Server	File Server IP Address. Subtype = 6.

Table continues…

Category	TLV Name (Type)	TLV Info String (Value)
Avaya Proprietary	802.1Q Framing	802.1Q Framing = 1 if tagging or 2 if not.
Basic Mandatory	End-of-LLDPDU	Not applicable.

TLV impact on system parameter values

System parameter name	TLV name	Impact
PHY2VLAN	IEEE 802.1 Port VLAN ID	The value of the PHY2VLAN parameter on the phone is configured from the value of the Port VLAN identifier in the TLV.
L2QVLAN and L2Q	IEEE 802.1 VLAN Name	The value is changed to the TLV VLAN Identifier. L2Q is set to 1 (ON). A check is made as to whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. VLAN Name TLV is ignored if: • The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0. • The current value of L2QVLAN was set by a TIA LLDP MED Network Policy TLV. • The VLAN name in the TLV does not contain the substring “voice” in lower-case, upper-case or mixed-case ASCII characters anywhere in the VLAN name.
L2Q, L2QVLAN, L2QAUD, DSCPAUD	TIA LLDP MED Network Policy (Voice) TLV	L2Q - set to 2 (off) if T (the Tagged Flag) is set to 0 and to 1 (on) if T is set to 1. L2QVLAN - Set to the VLAN ID in the TLV. L2QAUD - Set to the Layer 2 Priority value in the TLV. DSCPAUD - Set to the DSCP value in the TLV. A check is made as to whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. This TLV is ignored if: • The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0. • The Application Type is not 1 (Voice) or 2 (Voice Signaling). • The Unknown Policy Flag (U) is set to 1.

Table continues…

System parameter name	TLV name	Impact
L2Q, L2QVLAN	TIA LLDP MED Network Policy (Voice Signaling)	L2Q - set to 2 (off) if T (the Tagged Flag) is set to 0 and to 1 (on) if T is set to 1. L2QVLAN - Set to the VLAN ID in the TLV. L2QAUD - Set to the Layer 2 Priority value in the TLV. DSCPAUD - Set to the DSCP value in the TLV. A check is made as to whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. This TLV is ignored if: • The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0. • The Application Type is not 1 (Voice) or 2 (Voice Signaling). • The Unknown Policy Flag (U) is set to 1.
SIP_CONTROLLER_LIST	Proprietary Call Server TLV	SIP_CONTROLLER_LIST will be set to the IP addresses or FQDN in this TLV value. **Note:** This parameter cannot be used in an environment where both SIP phones and H.323 phones exist.
L2Q	Proprietary 802.1 Q Framing	If the value of TLV = 1, L2Q is set to 1 (On). If the value of TLV = 2, L2Q is set to 2 (Off). If the value of TLV = 3, L2Q is set to 0 (Auto). A check is made as to whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. This TLV is ignored if: • The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0. • The current L2QVLAN value was set by an IEEE 802.1 VLAN name. • The current L2QVLAN value was set by a TIA LLDP MED Network Policy (Voice) TLV.

Automatic phone provisioning using Device Enrollment Services

During initial boot-up, the phone prompts users to select if they want to contact the Device Enrollment Services server. The phone displays the `Do you want to activate Auto Provisioning now` prompt.

The user has 60 seconds to select **Yes** or **No** options, or the timeout is activated.

The following options are available:

- **Yes**: This option indicates that the phone should use only Device Enrollment Services for server discovery instead of a local network.

  If the phone can contact Device Enrollment Services and can obtain the configuration server URL, it contacts the configuration server to get the settings. If the phone fails to contact the configuration server, it prompts the user to enter the configuration server information manually.

  If the phone can contact Device Enrollment Services, but there is no configuration server assigned to the phone on Device Enrollment Services, it prompts the user to enter the numeric enrollment code.

  The numeric enrollment code is an 8 digit or 12 digit number as defined in Device Enrollment Services. For more information, see Device Enrollment Services administration documents at http://support.avaya.com/.

  When the user enters the numeric enrollment code, the phone contacts Device Enrollment Services again to obtain data on its configuration server and contacts the configuration server to download the settings.

  The user can cancel the operation of entering the numeric enrollment code. In this case, they are prompted to enter the configuration server manually.
- **No**: This option indicates that the phone should not use Device Enrollment Services and should discover the configuration server using the existing mechanism based on DHCP SSON, LLDP, PnP or Administration menu. If the phone fails to discover the configuration server using DHCP SSON, LLDP or PnP it prompts the user to enter the provisioning details manually.
- **Timeout**: After 60 seconds, if no option is selected, the phone uses the existing mechanism based on DHCP SSON, LLDP or PnP. If the phone fails to discover the configuration server, in this case, it contacts Device Enrollment Services to get the configuration server URL.

Related links

Automatic phone provisioning on page 32

Virtual LAN (VLAN)

VLANs provide a means to segregate your network into distinct groups or domains. They also provide a means to prioritize the network traffic into each of these distinct domains. For example,

a network may have a Voice VLAN and a Data VLAN. Grouping devices that have a set of common requirements has the following advantages:

- greatly simplifies network design
- increases scalability
- improves security
- improves network management

The networking standard that describes VLANs is IEEE 802.1Q. This standard describes in detail the 802.1Q protocol and how Ethernet frames get an additional four-byte tag inserted at the beginning of the frame. This additional VLAN tag describes the VLAN ID that a particular device belongs to and the priority of the VLAN tagged frame. Voice and video traffic typically get a higher priority in the network as they are subject to degradation caused by network jitter and delay.

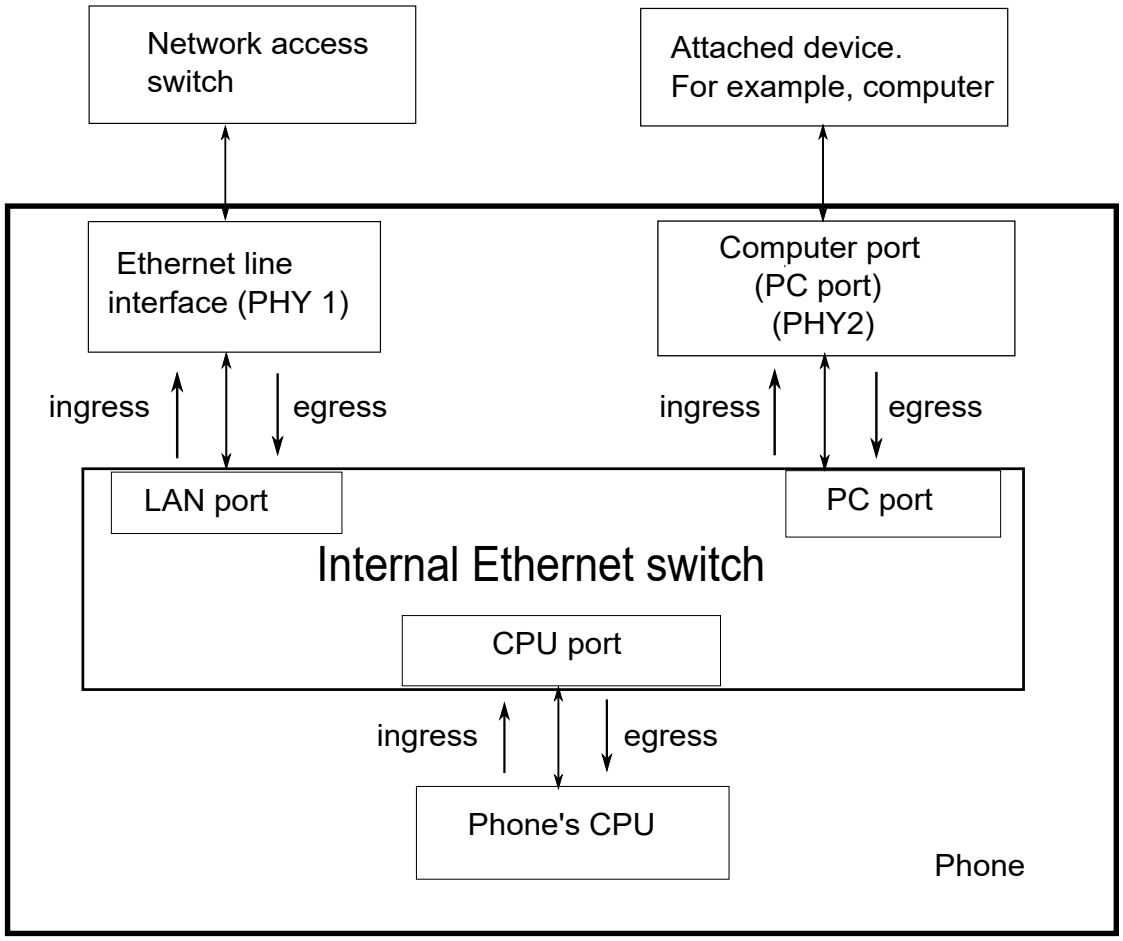
VLAN separation

The Avaya J100 Series IP Phones have an internal network switch that is capable of using VLANs to segregate traffic between the LAN port, the PC port and the internal port that goes to the CPU of the phone. You can have VLAN functionality on this switch and configure the switch to isolate the traffic destined for the CPU of the phone from that destined to the PC port.

Note:

Disable flow control on any device connected by PHY2.

The configuration of the internal switch of the phone can be done through the `46xxsettings.txt` file, LLDP or DHCP. It is preferable to configure the VLAN settings on the internal switch of the phone through DHCP or LLDP as these protocols are run prior to and during network initialization. If that is not possible then the `46xxsettings.txt` file configuration parameters can be used and the VLAN can be started in automatic mode which is the default mode.



VLAN separation modes

Avaya J100 Series IP Phones supports two VLAN separation modes:

- No VLAN separation mode: In this mode, the CPU port of the port receives untagged frames and tagged VLAN frames on any VLAN irrespective of whether the phone sends untagged or tagged frames. This traffic can be received from the PC port or LAN port. The filtering of the frames is done by the CPU itself. In order to reduce unnecessary traffic to the CPU, the administrator should configure only the necessary VLANs on the external switch port, in particular, voice VLAN and data VLAN.
- Full VLAN separation mode: This is the default mode. In this mode, the CPU port of the phone receives tagged frames with VLAN ID = L2QVLAN whether they are from the LAN port or the PC port. The PC port receives untagged or tagged frames with VLAN ID = PHY2VLAN from the LAN port. The PC port cannot send any untagged frames or tagged frames with any VLAN ID, including the voice VLAN ID, to the CPU. Frames received externally on the PC port can only be sent to the LAN port if they are untagged frames or tagged frames with VLAN ID= PHY2VLAN. In this mode, there is a complete separation between the CPU port and the PC port. In order to configure Avaya J100 Series IP Phones to work in this mode, all of the following conditions must be met:
  - VLANSEPMODE = 1 (default)

- L2Q = 0 (auto, default) or 1 (tag)
- L2QVLAN is not equal to 0
- PHY2VLAN is not equal to 0
- L2QVLAN is not equal to PHY2VLAN

In this mode, phone can send and receive Ethernet frames that are tagged voice VLAN ID (L2QVLAN). If there is a DHCP server on this LAN that is reachable by this phone, then this server can also send and receive tagged frames with the same VLAN ID.

If one of these conditions is not met then the phone works in no VLAN separation mode where all kinds of traffic reaches the CPU port of the phone.

Note:

The phone can send tagged VLAN frames on the voice VLAN (L2QVLAN), but still not work in full VLAN separation mode. For example, when PHY2VLAN = 0 or VLANSEPMODE = 0.

Configuring an external switch port

About this task

It is important to restrict the VLAN binding in no VLAN separation mode. This is because the internal phone switch does not filter the frames and the CPU of the phone is subjected to all the traffic going through the phone. In full VLAN separation mode, the internal phone switch filters any tagged VLAN frames with VLANs other than voice VLAN and data VLAN. However, you must configure only the necessary VLANs on the external switch port.

Procedure

1. Bind VLAN to the voice VLAN, that is L2QVLAN, and the data VLAN, that is PHY2VLAN.
2. Set the default VLAN as the data VLAN.

   This data VLAN is the VLAN assigned by the external switch port to untagged frames received from the phone LAN port.
3. Configure one of the following for egress tagging:
   - Data VLAN is untagged and voice VLAN is tagged.
   - Data VLAN and voice VLAN are both tagged. You must configure this option to have full VLAN separation.

   When egress voice VLAN frames are sent untagged from the external switch port to the phone LAN port, there is no VLAN separation between the voice VLAN and data VLAN.

Exceptions to the VLAN forwarding rules

Exceptions to the VLAN forwarding rules are as follows:

- LLDP frames are always exchanged between the following in all VLAN separation modes:
  - The LAN port and CPU port
  - The CPU port and LAN port
- Spanning tree frames are always exchanged between the LAN port and PC port in all VLAN separation modes.
- 802.1x frames are always exchanged between the following in all VLAN separation modes according to DOT1XSTAT and DOT1X configuration:
  - The LAN and CPU port or PC port
  - The PC and CPU port or LAN port
  - The CPU port and LAN port

Special considerations

Special use of VLAN ID=0

The phone adds a VLAN tag to the egress voice frames with a VLAN ID=0 in certain configurations. For example, to utilize the priority functionality of the VLAN frame only and not the VLAN ID properties. In this case, use the parameter L2QAUD or L2QSIG to set the value of the VLAN priority portion of the VLAN tag.

Automatic failback of VLAN tagging

The phone connects to a network when the value of L2QVLAN does not match with the VLAN being assigned to the network access switch. When the phone starts to connect, it tries to contact the DHCP server with a VLAN ID=L2QVLAN. If the phone does not receive a DHCPOFFER with that particular VLAN ID, then it eventually fails back. The phone tries to contact the DHCP server again if L2Q is set to 0 and the VLAN tag is not set.

The VLANTEST parameter determines how long the phone waits for a recognizable DHCPOFFER. If VLANTEST is set to 0, then the phone does not fail back and keeps sending DHCP requests by using tagged VLAN frames with VLAN ID = L2QVLAN.

VLAN support on the computer or PC port

In full VLAN separation mode, the phone only supports one VLAN on the computer port. In no VLAN separation mode, all VLANs pass between the LAN and PC ports. However, the CPU port receives all traffic even if on VLANs that are not equal to L2QVLAN.

VLAN parameters

The following tables lists the parameters which are used to configure VLAN functionality on the network switch internal to the phone:

Parameter name	Default value	Description
L2Q	0	Specifies if layer 2 frames generated by the telephone have IEEE 802.1Q VLAN tags. Value operation: • 0: Auto. VLAN tagging is turned on when the network can support VLAN tagging and L2QVLAN is non zero. • 1: On. VLAN tagging is turned on when the network can support VLAN tagging. The IP phone sends tagged frames with VLAN = L2QVLAN, even if L2QVLAN is set to 0. • 2: Off. VLAN functionality is disabled. L2Q is configured through: • Local admin procedure • A name equal to value pair in DHCPACK message • SET command in a settings file • DHCP option 43 • LLDP
VLANTEST	60	Specifies the number of seconds that the phone waits prior to failing back to a different VLAN ID if no response is received from the DHCP server. Valid values are 0 through 999. Value operation: • 0: The phone continues to attempt a DHCP REQUEST forever. VLANTEST is configured through: • Settings file • A name equal to value pair in DHCPACK message

Table continues…

Parameter name	Default value	Description
VLANSEP	1	Specifies whether the VLAN separation is enabled or disabled by the built-in Ethernet switch. Value operation: • 0: Disabled • 1: Enabled
VLANSEPMODE	1	Specifies whether the VLAN separation is enabled or disabled. Value operation: • 0: Disabled • 1: Enabled VLANSEPMODE is configured through the settings file.
PHY2TAGS	0	Determines whether or not VLAN tags are stripped on Ethernet frames going out of the Computer (PC) port. Value operation: • 0: Strip tags. VLAN tags are stripped from Ethernet frames leaving the computer (PC) port of the phone. • 1: Does not strip tags. VLAN tags are not stripped from Ethernet frames leaving the Computer (PC) port of the phone. PHY2TAGS is configured through the settings file.

Table continues…

Parameter name	Default value	Description
L2QVLAN	0	Specifies the voice VLAN ID to be used by IP phones. Valid values are 0 through 4094. L2QVLAN is configured through: • Local admin procedure • A name equal to value pair in DHCPACK message • SET command in a settings file • DHCP option 43 • LLDP
PHY2VLAN	0	Specifies the value of the 802.1Q VLAN ID used by frames forwarded to and from the secondary (PHY2) Ethernet interface when VLAN separation is enabled. Valid values are 0 through 4094. PHY2VLAN is configured through: • SET command in a `settings` file • LLDP
L2QAUD	6	Specifies the value of the VLAN priority portion of the VLAN tag when the phone generates tagged Ethernet frames from the internal CPU of the phone. These values are inserted into the VLAN tag for audio frames (RTP, RTCP, SRTP, SRTCP). All other frames except those specified by the L2QSIG parameter are set to priority 0. Valid values are 0 through 7. L2QAUD is configured through: • SET command in a settings file • LLDP

Table continues…

Parameter name	Default value	Description
L2QSIG	6	Specifies the layer 2 VLAN priority value for signaling frames generated by the phone. Valid values are 0 through 7. L2QSIG is configured through: • SET command in the `Settings` file • AADS • LLDP Setting this parameter through AADS or LLDP overwrites values in the settings file.

TCP and UDP ports

Avaya J100 Series IP Phones use different protocols, such as TCP and UDP to communicate with other equipment in the network. Part of this communication identifies which TCP or UDP ports each piece of equipment uses to support each protocol and each task within the protocol. Depending on your network, you need to know what ports or ranges are used in the operation of the phones.

Related links

Received packets (destination = SIP phone) on page 69

Received packets (destination = SIP phone)

Destination port	Source port	Use	Protocol UDP or TCP
The number used in the Source Port field of the packets that the HTTP client of the phone sends	Any	Packets that the HTTP client of the phone receives	TCP
The number used in the Source Port field of the SSL packets that the HTTP client of the phone sends	Any	SSL packets that the HTTP client of the phone receives	TCP

Table continues…

Destination port	Source port	Use	Protocol UDP or TCP
68	Any	Received DHCP messages	UDP
SIP messages initiated by the call server should be sent to the port number specified by the value of SIPPORT (TCP). Responses to SIP messages initiated by the phone should be sent to the number used in the Source Port field of the message from the phone.	Any	Received signaling protocol	TCP
The number used in the Source Port field of the DNS query that the phone sends	Any	Received DNS messages	UDP
The number used in the Source Port field of the SNTP query that the phone sends	Any	Received SNTP messages	UDP
161	Any	Received SNMP messages	UDP

Related links

TCP and UDP ports on page 69

Transmitted packets (source = SIP phone)

Destination port	Source port	Use	Protocol UDP or TCP
53	Any unused port number	Transmitted DNS messages	UDP
67	68	Transmitted DHCP messages	UDP
80, unless explicitly specified otherwise	Any unused port number	Packets transmitted by the HTTP client of the phone	TCP
123	Any unused port number	Transmitted SNTP messages	UDP

Table continues…

Destination port	Source port	Use	Protocol UDP or TCP
The number used in the Source Port field of the SNMP query packet received by the phone	161	Transmitted SNMP messages	UDP
443, unless explicitly specified otherwise	Any unused port number	TLS/SSL packets transmitted by the HTTP client of the phone.	TCP
514	Any unused port number	Transmitted Syslog messages	UDP, TLS for secure syslog
The port number specified in the test request message	50000	Transmitted SLA Mon™ agent test results messages	UDP
System-specific	Any unused port number	Transmitted signaling protocol packets	TCP
FEPORT + 1 (if FEPORT is even) or FEPORT -1 (if FEPORT is odd) or the port number specified in a CNA RTP test request plus or minus one, as with FEPORT	PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd) or the port number reserved for CNA RTP tests plus or minus one, as for PORTAUD, above	RTCP packets transmitted to the far-end of the audio connection	UDP
RTCPMONPORT	PORTAUD + 1 (if PORTAUD is even) or PORTAUD – 1 (if PORTAUD is odd)	RTCP packets transmitted to an RTCP monitor	UDP
System-specific	Any unused port number	Transmitted signaling protocol packets	UDP

Session Traversal Utilities for NAT overview

A SIP phone (Host, Client) operating behind a Network Address Translator (NAT) has a private IP address and separate ports for each of the SIP signaling, RTP and RTCP ports.

When the phone first sends a data packet from its private address and some private port through the NAT, the NAT allocates a corresponding public IP address and port (known as a binding) that external peers can use to communicate with the phone.

Session Traversal Utilities for NAT (STUN) is a set of methods that allow the phone to discover its public IP address and ports for SIP signaling, RTP and RTCP.

Periodic traffic, or keep-alives, must be sent from the phone's active private ports to refresh the NAT bindings so that the NAT will not terminate them due to inactivity.

For Avaya J100 Series IP Phones, the STUN functionality is supported only in Open SIP environments.

Using a STUN Binding Request and Response

The phone performs STUN discovery of its public SIP signaling IP address and port at registration time. For public RTP and RTCP address and ports, the phone performs STUN discovery every time a call is established.

The following describes how the phone uses STUN to create a NAT binding and discover the corresponding public IP address and the port:

- Through NAT, the phone sends a STUN Binding Request from its private SIP signaling, RTP or RTCP source IP address and port to the STUN server. This creates a NAT binding.
- NAT overwrites the private source IP address and port of the packet IP header with the bound public IP address and the port.
- The STUN server replies with a STUN Binding Response containing the public source IP address and the port received from NAT.
- NAT routes the STUN Binding Response back to the phone private IP address and the port.

STUN limitations

The following are the limitations for using the STUN functionality:

- Symmetric NAT is not supported.
- NAT traversal mechanisms must support Network Address Port Translation (NAPT). See RFC 3022 *Traditional IP Network Address Translator (Traditional NAT)* for more details.
- NATs must support hairpinning to allow the phones behind the same NAT to communicate. See RFC 4787 *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP* for more details.
- Only unauthenticated STUN is supported.
- When the STUN feature is activated, SIP ALG functionality must be disabled for NAT traversal mechanisms.

Related links

STUN parameters on page 72

STUN parameters

The following tables lists the parameters which are used to configure the STUN functionality:

Parameter name	Default value	Description

STUN_SERVER_ADDRESS	N/A	This is the basic STUN parameter defining the STUN server address. Other parameters listed below will be ignored if this parameter is not set.
		
		The valid value is an IPv4 address in the dotted decimal format or a FQDN.
		
		Note:
		
		If specified as an IPv4 address, the STUN server port will default to 3478.
		
		The following characters are allowed:
		
		• 0 – 9
		• a – z
		• A – Z
		• dot (“.”)
		
		For example,
		`SET STUN_SERVER_ADDRESS 192.168.161.54`
		
		or
		`SET STUN_SERVER_ADDRESS domain.com`

STUN_UDP_INITIAL_TIMEOUT_MSEC	500	Determines the initial timeout, in milliseconds, to wait for a Response to a STUN Request sent over UDP. The timeout value is internally doubled after each (re)transmission. Valid values are positive integers from 500 (0,5 sec) to 3000 (3 sec).
STUN_UDP_MAX_TRANSMISSIONS	7	Sets the number of times the phone will transmit a STUN Request until a Response is received, after which the Request will be treated as failed. Valid values are positive integers from 1 to 7.

Table continues…

Parameter name	Default value	Description
STUN_UDP_MAX_MEDIA_TRANSMISSIONS	3	Specifies the number of times the phone transmits a STUN Request to get NAT bindings for the phone's RTP or RTCP IP address and ports. Retransmissions continue until a response is received, or until the total number of requests has been sent. Initial timeout, in milliseconds, to wait for a Response to a STUN Request sent over UDP for media is 500 msec. The timeout value is internally doubled after each (re)transmission. Valid values are 1 through 4.
NAT_SIGNALING_KEEPALIVE_ENABLED	1	Determines whether the telephone sends keep-alives to refresh NAT bindings for the phone's private signaling IP address and port. Valid values: • 0: Keep-alive messages are not sent. • 1: Keep-alive messages are sent.
NAT_SIGNALING_KEEPALIVE_OVERRIDE_SEC	29	Sets the interval, in seconds, between keep-alives used to refresh NAT bindings for the phone signaling IP address and port. Valid values: • None: The phone will use the default value. • 15 – 900: The phone will use this value as the keep-alive interval for every SIP registration and dialog.

Related links

Session Traversal Utilities for NAT overview on page 71

IPv4 and IPv6

Avaya J100 Series IP Phones support IPv4 and IPv6 dual mode, as well as only IPv6 mode. All the IPv4 functionality is retained for IPv6. IPv6 protocol is enabled by default.

Avaya J100 Series IP Phones support the following combinations of IPv4 and IPv6 IP address configuration:

- Dual mode: Both IPv4 and IPv6 addresses are configured by using static addressing.
- Dual mode: Both IPv4 and IPv6 addresses are configured by using DHCP.
- IPv4 only mode.

Configuring IPv4 from the phone menu

About this task

Use this procedure to configure DCHPv4 from the phone Ethernet IPv4 menu. In this menu, you can also view the phone IPv4 address, gateway and mask IPv4 addresses.

Note:

If you disable **Use DHCP** option, manual input mode will be enabled.

Before you begin

Obtain the access code to Administration menu.

Procedure

1. On the phone, press **Main Menu**.
2. Scroll to **Administration**, and press **Select**.
3. In the **Access code** field, enter the administration password.

   The default access code is `27238`.
4. Press **Enter**.
5. Scroll to **IP Configuration**, and press **Select**.
6. Scroll to **Ethernet IPv4**, and press **Select**.
7. Scroll to **Use DHCP**, and press **Toggle** to enable or disable DCHPv4.
8. Press one of the following:
   - **Save**
   - **OK**
9. **(Optional)** Press **Cancel** to exit the menu without saving the changes.

Configuring IPv4 from the web interface

Before you begin

Obtain the access code to Administration menu.

On the phone, use Administration menu for the following:

- Enable the web server.
- Get the IP address of the phone.

See Enabling access to the web interface through the Administration menu of the phone on page 116 and Viewing IP address of the phone on page 117 for more details.

Procedure

1. In your browser, enter the IP address of the phone, and press **Enter**.
2. On the Login page, enter the username and the password in the corresponding fields.

   For more information about changing the default password, see Logging in to the phone web interface on page 117.
3. Navigate to **IP Configuration** > **IPv4 Configuration (Ethernet)**.
4. Configure IPv4 addresses in the following way:
   - To enable DHCPv4, select **Yes** from the drop-down menu next to the **Use DHCP** option.
   - Enter the required values in **IPv4 Address**, **Subnet Mask** and **IPv4 Gateway** fields.
5. Scroll to the end of the Ethernet page, and press **Save**.

Configuring a DHCP server in the dual and IPv6-only environments

About this task

In the dual (IPv4 and IPv6) and IPv6-only environments, the phone acquires vendor-specific parameters, including the IP address of the file server, through DHCPv6 vendor-specific option 17. Use this procedure to set this option with an opt-code 242 to obtain an IPv6 address for the file server.

Before you begin

In the dual environment, install the DHCPv4 and DHCPv6 server software according to instructions provided by your vendor.

In the IPv6-only environment, install the DHCPv6 server.

Procedure

1. Depending on the environment, do one of the following:
   - In the dual environment, specify the IP address of the file server using DHCPv4.
   - In the IPv6-only environment, specify the IP address of the file server using DHCPv6.
2. Configure the DHCPv6 server to send a Vendor-Specific Information (VSI) option with an enterprise number of 6889 which is the Avaya Enterprise Number.
3. Include the vendor-specific option 17 with an opt-code of 242 within that option.
4. Set the option-data portion of the vendor-specific option with the HTTPSRVR parameter.

Example

The following shows an example of setting the vendor-specific option 17 in the `dhcp6.conf` file:

```
## SSON on Avaya phone default is 242
## Specific the HTTP server used by the Avaya phones

## Allocate 2 bytes for option code, 2 bytes for option data length, 3 hash buckets
option space Avaya code width 2 length width 2 hash size 3;
option Avaya.avaya-option-242 code 242 = text;

## 6889 is enterprise number for Avaya
option vsio.Avaya code 6889 = encapsulate Avaya;

## option data (sample):
option Avaya.avaya-option-242
"HTTPSRVR=2000::114f:85f7:f238:9eb5,MCIPADD=2000::54,SIG=SIP";
```

Next steps

In the dual environment, it is recommended to set DUAL_IPPREF to 6 to override the default value of 4 in the `46xxsettings.txt` file.

This parameter is used only in dual mode to apply Site Specific Option Number (SSON) parameters either from a DHCPv4 or a DHCPv6 server.

IPv6 configuration

Use the `46xxsettings.txt` file to set the following parameters for IPv6 operation:

Parameter name	Default value	Description
DHCPSTDV6	0	Specifies whether DHCPv6 will comply with the IETF RFC 8415 standard and immediately stop using an IPv6 address if the address valid lifetime expires, or whether it will enter an extended rebinding state. Value operation: • 0: DHCPv6 enters proprietary extended rebinding state (continue to use IPv6 address, if DHCPv6 lease expires). • 1: DHCPv6 complies with IETF RFC 8415 standard (immediately release IPv6 address, if DHCPv6 lease expires).
DUAL_IPPREF	4	DUAL_IPPREF controls the following: • The selection of SSON either from DHCPv4 or DHCPv6 server, when phone is in dual mode, and • 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. Value operation: • 4(Default): IPv4 is preferred. • 6: IPv6 is preferred.

Table continues…

Parameter name	Default value	Description
PRIVACY_SLAAC_MODE	1	Specifies the preference for Privacy Extensions. Value operation: • 0: Disable Privacy Extensions. • 1(Default): Enable Privacy Extensions, and prefer public addresses to temporary addresses. • 2: Enable Privacy Extensions, and prefer temporary addresses to public addresses.
IPV6STAT	1	Specifies the mode of the IP family which will be used in the current configuration. Value operation: • 0: Only IPv4 mode is enabled. • 1(Default): Dual mode is enabled. • 2: Only IPv6 mode is enabled.
IPV6DADXMITS	1	Specifies whether Duplicate Address Detection is performed on tentative addresses, as specified in RFC 4862. Value operation: • 0: DAD is disabled • 1 to 5: Maximum number of transmitted Neighbor Solicitation messages.

Configuring IPv6 from the phone menu

About this task

Use this procedure to configure IPv6 addresses from the phone Ethernet IPv6 menu. In this menu, you can also view the phone IPv6 address, gateway address and prefixes if configured.

Note:

If you disable **Use DHCP** option, manual input mode will be enabled after rebooting the phone.

Before you begin

Obtain the access code to Administration menu.

Procedure

1. On the phone, press **Main Menu**.
2. Scroll to **Administration**, and press **Select**.
3. In the **Access code** field, enter the administration password.

   The default access code is `27238`.
4. Press **Enter**.
5. Scroll to **IP Configuration**, and press **Select**.
6. Scroll to **Ethernet IPv6**, and press **Select**.
7. Do one of the following:
   - Configure as required **Use DHCP(V6)** or **Use SLAAC** fields by pressing **Toggle**.
   - Enter IPv6 addresses manually in **Phone(v6)** and **Gateway(v6)** fields.
8. Press one of the following:
   - **Save**
   - **OK**
9. **(Optional)** Press **Cancel** to exit the menu without saving the changes.

Configuring IPv6 from the web interface

Before you begin

Obtain the access code to Administration menu.

On the phone, use Administration menu for the following:

- Enable the web server.
- Get the IP address of the phone.

See Enabling access to the web interface through the Administration menu of the phone on page 116 and Viewing IP address of the phone on page 117 for more details.

Procedure

1. In your browser, enter the IP address of the phone, and press **Enter**.
2. On the Login page, enter the username and the password in the corresponding fields.

   For more information about changing the default password, see Logging in to the phone web interface on page 117.
3. Navigate to **IP Configuration** > **IPv6 Configuration (Ethernet)**.

4. Configure IPv6 addresses in the following way:
   - To enable DHCPv6, select **Yes** from the drop-down menu next to the **Use DHCPv6** option.
   - To use SLAAC addresses, select **Yes** from the drop-down menu next to the **Use SLAAC** option.
5. Scroll to the end of the Ethernet page, and press **Save**.

IPv6 limitations

After upgrading Avaya J100 Series IP Phones to the current release firmware version, if IPv6 was not enabled previously, the phone will function in dual mode to get valid IPv6 address from the network. This may cause an additional reboot of the phone.

Microsoft® Exchange account integration

You can integrate the Avaya J100 Series IP Phones except for Avaya J129 IP Phone with the Microsoft® Exchange account by using the Microsoft® authentication method. After successful authentication, the user's Exchange calendar and contacts are integrated with the phone. You can choose to integrate the phone or provide the access to the phone user. You can use one of the following to integrate the phone:

- `46xxsettings.txt`
- Phone web interface

The user can integrate the calendar application in their new out-of-the-box phone by using the Oauth or basic authentication. For basic authentication of the new phone, you must set the parameters EXCHANGE_EMAIL_DOMAIN and EXCHANGE_AUTH_USERNAME_FORMAT in the `46xxsettings.txt` file.

Related links

Microsoft Exchange account integration configuration parameters on page 81

Microsoft Exchange account integration configuration parameters

Use `46xxsettings.txt` file to set the following parameters:

Parameter name	Default Value	Description
EXCHANGE_SERVER_LIST	outlook.office365.com	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.
EXCHANGE_SERVER_SECURE_MODE	1	Specifies if HTTPS should be used to contact Exchange servers. Value operation: • 0: Use HTTP • 1: Use HTTPS **Note:** Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default Value	Description
EXCHANGE_AUTH_METHOD_DEFAULT	0	Specifies the Exchange authentication method configured by administrator. When you configure Basic (Forced) or OAuth (Forced) method, it is the active authentication method. The phone user is not allowed to change the authentication method from phone user interface. When you configure non-forced method, phone user can change the authentication method from the phone user interface and configure the active authentication method. Value operation: • **0**: Basic authentication (Default) • **1**: OAuth authentication • **2**: Basic authentication- forced • **3**: OAuth authentication- forced **Note:** Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default Value	Description
EXCHANGE_AUTH_USERNAME_FORMAT	0	Specifies the necessary format of the username for http authentication. Value operation: • 0: Office 2003/Office2016 username format. Username=<ExchangeUserDomain\ExchangeUserAccount> or Username=<ExchangeUserAccount> if <ExchangeUserDomain> is empty. • 1: Office 365 format. Username=<ExchangeUserAccount@ExchangeUserDomain> or Username=<ExchangeUserAccount> if <ExchangeUserDomain> is empty.
EXCHANGE_USER_ACCOUNT_DEFAULT	Null	Specifies the Exchange user account configured by administrator. This parameter is only applicable when authentication method is OAuth. If phone user hasn't configured any user name on the phone user interface then value configured in this parameter would be used. The valid value is a string of up to 255 characters. The default value is empty. **Note:** Avaya J129 IP Phone does not support this feature.
EXCHANGE_EMAIL_DOMAIN	Null	Specifies the Exchange email domain. The value can contain 0 to 255 characters.

Table continues…

Parameter name	Default Value	Description
EXCHANGE_NOTIFY_SUBSCRIPTION_PERIOD	180	Specifies the number of seconds between re-syncs with the Exchange server. Valid values are 0 through 3600.
EXCHANGE_USER_DOMAIN	Null	Specifies the domain for the URL used to obtain Exchange contacts and calendar data. The parameter is used as a part of the user authentication. The value can contain 0 to 255 characters.

Related links

Microsoft Exchange account integration on page 81

Chapter 5: Open SIP operation modes

Avaya J100 Series IP Phones support configuration of specific Open SIP call servers. In an Open SIP environment, you can configure the phones in one of the following modes:

- Generic: Default Open SIP mode that provides basic call functionalities. The phones can connect to all the supported servers but cannot provide advanced call server functionalities. Avaya J100 Series IP Phones currently support FreeSWITCH, Metaswitch, Asterisk, Broadsoft, Netsapiens, and Avaya Cloud Office™ call servers.
- BroadSoft: The phones can connect to the Broadsoft call server and provide advanced functionalities.
- Netsapiens: The phones can connect to the Netsapiens call server. Currently, Netsapiens supports basic call functionalities.
- Avaya Cloud Office™: The phones can connect to the Avaya Cloud Office™ call server.

You can choose the required operation mode using the `46xxsettings.txt` file or the phone web interface.

Related links

Configuring an Open SIP operation mode through the settings file on page 86
Configuring an Open SIP operation mode through the web interface on page 87

Configuring an Open SIP operation mode through the settings file

In the `46xxsettings.txt` file, set the following parameters to the required value:

Parameter name	Default value	Description
ENABLE_3PCC_ENVIRONMENT	1	Specifies whether the phone is currently deployed in an Open SIP environment. In an Open SIP environment, the phones can be configured with a supported call server. Options: • 0: Non-Open SIP environment. The phones cannot be configured with an Open SIP call server. • 1: Open SIP environment. You can configure the phones with a supported Open SIP call server.
3PCC_SERVER_MODE	0	Specifies the Open SIP server mode. The parameter is applicable only if ENABLE_3PCC_ENVIRONMENT is set to 1. The options are: 0: The phone connects to any call server but provides only basic call functionalities. 1: The phone connects to the BroadSoft server mode. 3: The phone connects to the Netsapiens server mode. 5: The phone connects to the Avaya Cloud Office™ server mode. **Note:** Avaya J100 Series IP Phones do not support values 2 and 4. To connect to the RingCentral® server, set the value to 5.

Related links

Open SIP operation modes on page 86

Configuring an Open SIP operation mode through the web interface

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Environment Settings**.

3. In the Environment Setting section, do the following:
   - **AURA environment**: Disable the value.
   - **Discover AVAYA environment**: Disable the value.
   - **IP Office Environment**: Disable the value.
   - **3PCC Environment**: Enable the value.
   - **3PCC Server Mode**: Select the required operation mode.
4. Click **Save**.

Related links

Open SIP operation modes on page 86

Broadsoft configuration

BroadSoft server mode

The phone supports a basic and advanced set of features and functionalities in the BroadSoft mode.

In the BroadSoft operation mode, to configure Avaya J100 Series IP Phones, you can use the following:

- BroadSoft Device Management System
- Xtended Service Interface (Xsi)

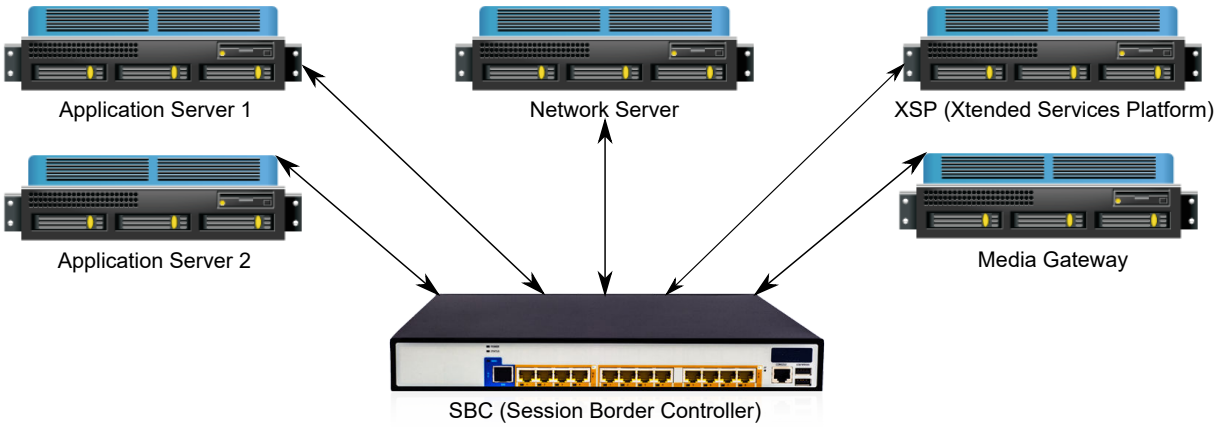
For more information about configuring Avaya J100 Series IP Phones for the BroadSoft server, see https://supportcenter.broadsoft.com/.

Related links

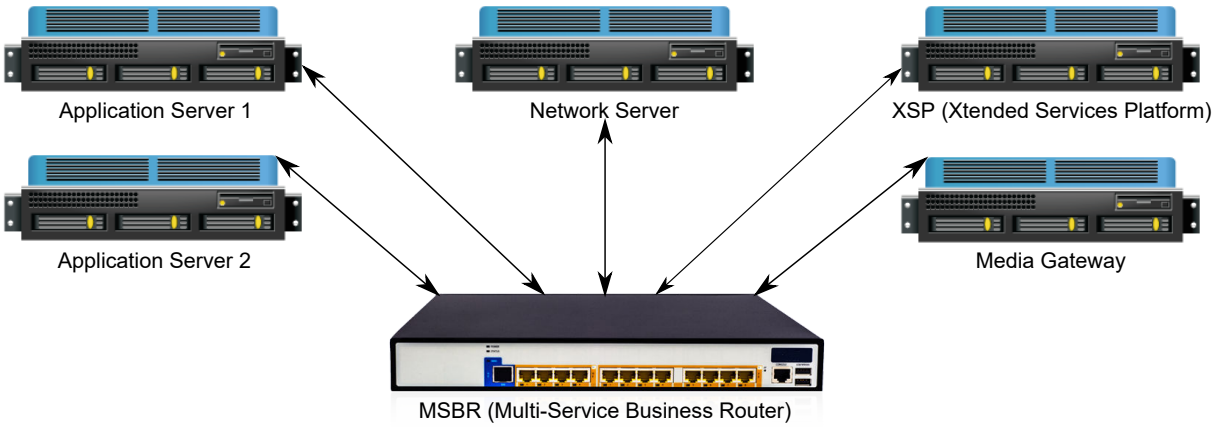
Open SIP operation modes on page 86

Broadworks topology

Broadworks topology with SBC



Broadworks topology without SBC



Related links

Open SIP operation modes on page 86

Broadsoft Device Management

With the Broadsoft Device Management feature, you can download device-specific configuration files from the Broadsoft server in Avaya J100 Series IP Phones. The phone uses the Broadsoft Device Management feature as the provisioning server.

Avaya J100 Series IP Phones support the following types of Broadsoft Device Management authentication:

- MAC-based authentication.
- HTTP digest authentication.
- TLS mutual authentication.

Device management configuration

The following initial configuration parameters should be set for the Broadsoft Device Management:

Parameter name	Default Value	Description
ENABLE_3PCC_ENVIRONMENT	1	Specifies whether the deployment environment is an Open SIP server. Value operation: • 0: Avaya environment. • 1 (Default): Open SIP environment.
3PCC_SERVER_MODE	0	Specifies if the phone expects a generic Open SIP server or a BroadSoft server (applicable when ENABLE_3PCC_ENVIRONMENT is set to 1). Value operation: • 0 (Default): Generic. • 1: BroadSoft.
ENABLE_OOD_RESET_NOTIFY	0	Specifies whether the phone supports Out Of Dialog (OOD) SIP NOTIFY message with Event:resync or Event:check-sync only. Value operation: • 0 (Default): OOD is not supported. • 1: OOD is supported. To support Broadsoft Device Management, this value should be set to 1.

Table continues…

Parameter name	Default Value	Description
XSI_URL	Null	Specifies BroadWorks Xtended Service Platform (XSP) server FQDN/IP address, HTTP or HTTPS mode and port. If the port is not defined, 80 is used for HTTP and 443 for HTTPS by default. This is the main parameter to make features work in BroadSoft environment. **Note:** If XSI_URL is defined, some local call features are not available. They must be enabled for the user on the BroadSoft server. For more information about XSI, see BroadSoft XSI support on page 269.

Chapter 6: Phone configuration

Avaya J100 Series IP Phones can be configured by using one of the following methods:

- the Administration menu on the phone
- the web interface of the phone Administration menu
- `46xxsettings.txt` file

You can configure the phone keys using the Pre-configuration of keys and soft keys using Soft key configuration.

Related links

Configuring the phone using Administration menu on page 93
Configuring the phone using the web interface on page 115
Configuring the phone using the settings file on page 217
Pre-configuration of keys on page 221
Soft key configuration on page 224

Configuring the phone using Administration menu

The Administration menu can be accessed from the Main Menu of the phone. For more information about accessing the Administration menu, see Accessing the Admin menu after log in on page 94.

The Administration menu contains the following sections:

- IP Configuration
- Debug
- Network interfaces
- Group
- Log
- Log Out
- Ping
- Get updates
- Reset to defaults

- Restart phone
- SIP
- SSON
- View
- Update info
- 802.1X
- Signaling
- Web server

Note:

When changed, some of the parameters require the phone reboot after exiting the Administration menu or immediate reboot. You will get the notification when configuring the parameters which need the phone reboot.

Accessing the Admin menu during phone startup

Before you begin

Ensure you set the following parameters in the `Settings` file:

- PROCSTAT: To administer the phone using admin menu, set the parameter to zero.
- PROCPSWD or ADMIN_PASSWORD: The default password is `27238`. You must change the default password at the time of initial installation.

Procedure

1. Press **Main Menu** soft key.
2. Scroll and select **Administration** soft key.
3. On the Access code screen, enter the admin menu password using the dialpad.
4. Press **Enter**.

Accessing the Admin menu after log in

Procedure

1. Navigate to **Main Menu** > **Administration**.
2. In the **Access code** field, enter the administration password.

   The default access code is `27238`.
3. Press **Enter**.

Related links

Accessing Admin Menu

Accessing the Ethernet IPv4 settings

Procedure

1. Navigate to **Main Menu** > **Administration**.
2. In the **Access code** field, enter the administration password.

   The default access code is `27238`.
3. Press **Enter**.
4. Select **IP Configuration**.

   The phone displays the parameters for IP configuration.

Related links

Accessing the Admin menu after log in on page 94

IP configuration field description

Configuration Parameter Name	Description
The following parameters are available in Ethernet IPv4 menu:	
Use DHCP	Specifies the access to view or manually enter the IP address. Press the **Toggle** button to make a selection.
Phone	Specifies the IP address of the phone. The available format is `nnn.nnn.nnn.nnn.`
Gateway	Specifies the gateway of the phone. The available format is `nnn.nnn.nnn.nnn.`
Mask	Specifies the network mask. The available format is `nnn.nnn.nnn.nnn.`
The following parameters are available in Wi-Fi IPv4 menu:	
SSID	Specifies the name of the Wi-fi network.
Use DHCP	Specifies the access to view or manually enter the IP address. Press the **Toggle** button to make a selection.
Phone	Specifies the IP address of the phone. The available format is `nnn.nnn.nnn.nnn.`
Gateway	Specifies the gateway of the phone. The available format is `nnn.nnn.nnn.nnn.`
Mask	Specifies the network mask. The available format is `nnn.nnn.nnn.nnn.`
The following parameters are available in the Servers menu:	

Table continues…

Configuration Parameter Name	Description
HTTPS	Specifies the IP address of the HTTPS file server. The available format is `addr1:8843/test`
HTTP	Specifies the IP address of the HTTP file server. The available format is `addr1:8080/test`
Username	Enter the provisioning server authentication user name.
Password	Enter the provisioning server authentication password.
DNS	Specifies the IP address of the DNS servers. The available format is `nnn.nnn.nnn.nnn.`
SNTP	Specifies the time server or servers settings.
STUN Server	Enter the IP address or fully qualified domain name of the STUN server address.
The following parameters are available in VLAN menu:	
802.1Q	Choose one of the following options: • **Auto**: Automatic mode. • **On**: Turns on the configuration. • **Off**: Turns off the configuration.
VLAN ID	Specifies the ID for VLAN. The available format is `dddd`.
VLAN test	Specifies the time in seconds, the phone waits for the DHCP server response. The available format is `ddd`.
The following parameters are available in Auto provisioning menu:	
Service	Specifies option for auto provisioning. Press **Toggle** to choose the required option: • **Inactive** • **Active**
Certificate	Specifies if the certificate is available.
Certificate Expiry	Specifies the expiry date of the certificate. The available format is `DD-MMM-YYYY`

Related links

SNTP server configuration on page 47

Signaling protocol

Signaling protocol is a type of communication protocol used for changing the signaling value to either SIP or H.323. Depending on the signaling value selected, it specifies the software used and controls the requests for the specific upgrade file.

Following are the methods used for changing the protocols for the enterprises requiring both H.323 and SIP-based protocols :

- The phone UI in the administration menu. Refer to Updating the signaling protocol in Related links.
- Updating the SIG parameter using:
  - The `46xxsettings.txt` file. Refer to Parameters for signaling protocol in Related links.
  - DHCP Option 242 (Site-Specific Option Number) or DHCP Option 43. See DHCP options in Related links.

When you change the protocol, there are few configuration parameters such as Group and SSON which are retained while upgrading to either SIP or H.323.

Note:

You must extract the software distribution package in the file server directory.

Related links

DHCP options on page 51
Updating the signaling protocol on page 97
Parameters for signaling protocol on page 98

Updating the signaling protocol

About this task

Use this procedure to set or update the Signaling Protocol in Avaya J100 Series IP Phones using the administration procedure when your environment has more than one protocol on a subnet. A valid SIG Protocol is **Default**, **SIP**, or **H.323**.

Note:

Perform this procedure only if the LAN Administrator instructs.

Procedure

1. Press **Main menu** > **Administration**.
2. In the **Access code** field, enter the admin menu password.
3. Press **Enter**.
4. Select **Signaling**.

   The signaling value is set to **Default**. The default value depends on the type of software to be used by the phone.

5. Press the **Toggle** softkey to see the other signaling options.

   The following **Signaling** values appear on the phone screen as you press the **Toggle** softkey.

   - **Default**
   - **SIP**
   - **H.323**

   If the current value is **SIP**, pressing the **Toggle** softkey changes the value to **Default**. If the current value is **H.323**, pressing the **Toggle** softkey changes the value to **SIP**.

6. Press **Save** to store the new setting and redisplay the Administration screen.

   The rest of this procedure depends on the status of the boot and application files.

Related links

Signaling protocol on page 97

Parameters for signaling protocol

Use `46xxsettings.txt` file to update the SIG parameter:

Parameter name	Default Value	Description
SIG	0	Specifies the type of software to be used by the phone 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 96x1 SIP software) or `J100Supgrade.txt` (for J100 SIP)

Related links

Signaling protocol on page 97

Using the debug mode

About this task

Use this procedure to activate or deactivate the debugging options.

Note:

If you use the default Administration menu password which is 27238, then many options in the Debug menu is read-only. You must reset the device Administration menu password to any non-default value to use all the options in the Debug menu.

Before you begin

You must set a HTTP server in the BRURI parameter in the `Settings` file that is capable of receiving a phone report from the phone. BRURI parameters can receive only phone report. It has no effect on any other debugging setting.

Procedure

1. Press **Main Menu** > **Administration**.
2. In the **Access code** field, enter the admin menu password.
3. Press **Enter**.
4. Select **Debug**.

   The phone displays the following debug options:

   - **Serial port mode**
   - **Port mirroring**
   - **Phone report**
   - **SSH access**
   - **SSH fingerprint**
   - **Clear SSH lockout**
   - **Service mode control**
   - **Service mode record**
5. Use the appropriate keys to enable or disable the options.
6. Press **Save**.

Related links

Accessing the Admin menu after log in on page 94

Setting the Ethernet interface control

Procedure

1. Press **Main Menu** > **Admin**.
2. In the **Access code** field, enter the admin menu password.
3. Press **Enter**.
4. Use the **Down Arrow** to select **Network interfaces**.

5. Use the **Right Arrow** key or the **Toggle** soft key to change the **Network mode** to **Ethernet** and do one of the following settings:
   - **Network config**: To change the network configuration to either Auto or Manual.
   - **Ethernet**: To change the Ethernet setting, go to step 6.
   - **PC Ethernet**: To change the PC Ethernet setting, go to step 7.
6. Use the **Right Arrow** key or the **Toggle** soft key to change the Ethernet setting to one of the following:
   - **Auto**
   - **10Mbps half**
   - **10Mbps full**
   - **100Mbps half**
   - **100Mbps full**
7. Use the **Right Arrow** key or the **Toggle** soft key to change the PC Ethernet setting to one of the following:
   - **Auto**
   - **10Mbps half**
   - **10Mbps full**
   - **100Mbps half**
   - **100Mbps full**
   - **Disabled**
8. Press **Save**.

Related links

Accessing the Admin menu after log in on page 94

Group identifier

You can assign a group identifier number to a community of IP phone users in an organization. The group identifier number ranges from 0 to 999. The default number is 0.

With a group identifier, you can apply a specific subset of configuration to a group of J100 devices within a settings file configuration. For example, you can group users by time zones or work activities. For more information about using the `46xxsettings.txt` file to configure Group, see Contents of the settings file.

You can configure the group identifier value using one of the following methods:

- The local administration process using the phone UI.
- The phone web interface.

Note:

After you set the Group identifier number to a non-zero value, to reset to zero, do one of the following:

- Reset the phone to default.
- Reset the value from the original source.

  For example, if you set a non-zero GROUP value in the phone web interface, reset the value to zero in the phone web interface.

Setting the group identifier

About this task

Use this procedure to set or change the group identifier only if the LAN Administrator instructs you to do so.

Procedure

1. Press **Main Menu** > **Administration**.
2. In the **Access code** field, enter the admin menu password.
3. Press **Enter**.
4. Select **Group**.
5. Enter any Group value between 0 to 999.

   When you change the Group value, the phone restarts after you exit the admin menu.
6. Press **Save**.

Related links

Accessing the Admin menu after log in on page 94

Setting event logging

About this task

Use the following procedure to enable or disable logging of system events.

Procedure

1. Press **Main Menu** > **Administration**.
2. In the **Access code** field, enter the admin menu password.
3. Press **Enter**.
4. Select **Log**.
5. Use the **Right** and **Left Arrow** keys to select one of the following values for the Log Level setting associated with the corresponding SYSLOG_LEVEL:
   - **Emergencies**: SYSLOG_LEVEL=0

- **Alerts**: SYSLOG_LEVEL=1
- **Critical**: SYSLOG_LEVEL=2
- **Errors**: SYSLOG_LEVEL=3
- **Warnings**: SYSLOG_LEVEL=4
- **Notices**: SYSLOG_LEVEL=5
- **Information**: SYSLOG_LEVEL=6
- **Debug**: SYSLOG_LEVEL=7

6. Scroll to **Log categories** and press **Select**.
7. Press **Toggle** and select the required Log Categories for the troubleshooting scenario.
8. **(Optional)** Scroll to **Remote logging enabled** and press **Toggle** to select.
9. **(Optional)** Scroll to **Remote log server** and enter the IP address or FQDN.
10. **(Optional)** Scroll to **Secure syslog** and press **Toggle** to select a secure or non-secure syslog mode.
11. Press **Save**.

Related links

Accessing the Admin menu after log in on page 94

Setting the dial plan

During automatic dialing, a dial plan allows a call to be initiated without using a **Send** button and without waiting for the expiration of a timeout interval. The dial plan consists of one or more format strings. When the dialed digits match a format string, the call is initiated. You can use one of the following methods to define dialed digit matching:

- DIALPLAN
- Digit mapping

Valid characters in a format string, and their meanings, are as follows:

- digits 0 through 9, inclusive = Specific dialpad digits
- * = the dialpad character *
- # = the dialpad character # (but only if it is the first character in the dialed string – see below)
- x = any dialpad digit (i.e., 0-9)
- Z or z = present dial tone to the user (for example, for Feature Access Code (FAC) entry)
- [ ] = any one character within the brackets is a valid match for a dial plan string
- - = any one digit between the bounds within the brackets, inclusive, is a match
- + = the character following the + can repeat 0 or more additional times, for a valid match

DIALPLAN

An individual valid dial plan is any combination of the above characters. If there are multiple valid dial plans, separate each one from the next using an OR symbol ("|"). If the dial plan text string begins or ends with an OR symbol, that symbol is ignored. Users cannot modify the dial plan.

Dial plan example:

"[2-4]xxx|[68]xxx|*xx|9Z1xxxxxxxxx|9z011x+"

where:

- [2-4]xxx: Four-digit dial extensions, with valid extensions starting with 2, 3, or 4;
- [68]xxx: Four-digit dial extensions, with valid extensions starting with 6 or 8;
- *xx: Two-digit Feature Access Codes, preceded by a *;
- 9Z1xxxxxxxxx: Network Access Code ("9 for an outside line"), followed by dial tone, followed by any string of 10 digits– typical instance of Automatic Route Selection (ARS) for standard US long distance number;
- 9z011x+: Network Access Code ("9 for an outside line"), followed by dial tone, followed by at least one digit – typical instance of Automatic Route Selection (ARS) for US access to international numbers of unknown, and variable, length.

Additional parameters that affect dialing are as follows:

- COUNTRY - Country of operation for specific dial tone generation.
- PSTN_VM_NUM (PSTN access number for Voice Mail system) - This parameter specifies the telephone number to be dialed automatically when the phone user presses the Messaging button under a non-AST controller. The phone places a PSTN call out from the local office and back in to the location that houses the voice mail server. Additional codes necessary to reach a specific user's voice-mail box may also be included. Example 1. SET PSTN_VM_NUM 96135550123
- ENABLE_REMOVE_PSTN_ACCESS_PREFIX - When the phone is operating with a non-AST controller and the value of the parameter is 0, the PSTN access prefix, defined by the parameter PHNOL, is retained in the outgoing number. If the value is 1, then the PSTN access prefix is stripped from the outgoing number.
- PHNLAC- A string representing the phone's local area code. When set, this parameter indicates the endpoint's local area code, which along with the parameter LOCAL_DIAL_AREA_CODE, allows users to dial local numbers with more flexibility. Example: SET PHNLAC 617
- LOCAL_DIAL_AREA_CODE- A flag indicating whether the user must dial the area code for calls within same area code regions. When the parameter is 0, the user does not need to dial the area code; when this parameter is 1, the user needs to dial the area code. When this parameter is enabled (1), the area code parameter (PHNLAC) should also be configured (i.e., not the empty string). Example: SET LOCAL_DIAL_AREA_CODE 1

Example 1- Setting the parameter configuration:

- SET ENHDIALSTAT 2
- SET PHNOL 27
- SET PHNCC 1

- SET PHNDPLENGTH 7
- SET PHNLDLENGTH 11
- SET PHNLD 0
- SET PHNIC 001

Table 1: : Example 2 In the Contacts list, save Contact X with the telephone number 41018989

PHNLAC Parameter Value	LOCAL_DIAL_AREA_CODE Parameter Value	Step to Execute	Result
020	1	Call X from Contacts list	Phone sends an invite message with 2702041018989.
020	1	Call X from Contacts list	Phone sends an invite message with 2741018989 and does not insert the local area code.
Null	1	Call X from Contacts list	Phone sends an invite message with 2741018989 and does not insert the local area code.

Restarting the phone

Procedure

1. Press **Main Menu** > **Administration**.
2. In the **Access code** field, enter the admin menu password.
3. Press **Enter**.
4. Select **Restart phone**.
5. Press **Restart** when the phone prompts for confirmation.

   A restart does not affect user-specified data and settings, such as contact data or the phone login and password.

Related links

Accessing the Admin menu after log in on page 94

Configuring Wi-Fi using phone UI

About this task

Use this procedure to configure a Wi-Fi network by using phone UI. Note that switching networks causes a reboot of the phone.

Procedure

1. Navigate to **Main Menu** > **Administration**.
2. In the **Access code** field, enter the administration password.

   The default access code is `27238`.
3. Press **Enter**.
4. Select **Network interfaces**.
5. Use the right arrow key or **Toggle** soft key to change **Network mode** to **Wi-Fi**.
6. Configure the following parameters:
   - **Network config**: Specifies if the WLAN is connected automatically or manually.
   - **SSID**: Specifies the network name for the WLAN you are using. Use the navigation key to select another SSID.
   - **Wi-Fi networks**: Displays available WLAN.
7. Use the navigation key to select a WLAN, and press **Connect**.
8. Press one of the following:
   - **Save**
   - **Cancel**
   - **Change**

Related links

Accessing the Admin menu after log in on page 94

Configuring SIP settings

About this task

Use this procedure to set up SIP-related settings, such as identifying the SIP proxy server.

Before you begin

To use TLS signaling, ensure ENFORCE_SIPS_URI is set to 0.

Procedure

1. Press **Main Menu** > **Administration**.
2. In the **Access code** field, enter the admin menu password.
3. Press **Enter**.
4. Select **SIP**.
5. Choose one of the following:
   - **SIP global settings**

- **SIP proxy list**

6. Press **Select** or **OK** to change any of the following SIP global settings:
   - **SIP domain**: Changes the domain parameter of SIP.
   - **Avaya environment**: Specifies whether the available SIP Avaya environment is in effect.

     The two modes are as follows:

     - **Auto**: Detects the Avaya environment automatically.
     - **Off**: Does not detect the Avaya environment and switches to a non-Aura mode.

     Note:

     This setting should always be Off for an Open SIP environment. Disable the Avaya Environment configuration from the `46xxsettings.txt` file.
   - **Registration policy**: Specifies the registration policy for SIP.

     The two modes are as follows:

     - **Alternate**: Supports registration to one of the active controllers.
     - **Simultaneous**: Supports registration to both the active controllers.
   - **Failback policy**: Specifies the fall back policy.

     The two modes are as follows:

     - **Auto**: Active controller automatically recovers after failback.
     - **Admin**: Active controller uses failback policy defined by the administrator.

     Note:

     Failback policy is not supported in an Open SIP setup.
   - **SIP proxy policy**: Specifies whether the settings of SIP proxy servers are taken from the `46xxsettings.txt` file or can be edited by the user.

     The two modes are as follows:

     - **Auto**: The settings are taken from the `46xxsettings.txt` file. The user can only view the settings in SIP Proxy Server menu.
     - **Manual**: The user can edit, delete, or create new server properties.
7. Select **SIP proxy list** to change SIP proxy list settings.

   Caution:

   Do not configure proxy settings manually while a user is logged in to the phone.

   The phone displays the IP address of the server that you selected.

8. Press **Select** and use the **Up** and **Down Arrow** keys to view, add, or change the following settings:
   - **SIP proxy**: Specifies the IP addresses or FQDN. The corresponding parameter is SIP_CONTROLLER_LIST.
   - **Protocol**: Specifies the type of protocol. The options are TLS, TCP or UDP. The corresponding parameter is SIP_CONTROLLER_LIST.

     Note:

     To set protocol UDP from the phone, set ENABLE_UDP_TRANSPORT using `46xxsettings.txt` file or the phone web interface.
   - **SIP Port**: Specifies the SIP port. If no value is entered, SIP port uses 5060 as the default port for UDP/TCP, or 5061 as the default port for TLS.

     Note:

     You cannot edit these values if the SIP Proxy Policy is in Auto mode.
9. Press **Save**.

Related links

Accessing the Admin menu after log in on page 94

Setting Site Specific Option Number (SSON)

About this task

The Site Specific Option Number (SSON) is used by the phones to request information from a DHCP server. This number must match a similar number option set on the DHCP server. The number option set on the DHCP server defines the various settings required by the phone.

Procedure

1. Press **Main Menu** > **Administration**.
2. In the **Access code** field, enter the administration menu password.
3. Press **Enter**.
4. Select **SSON**.
5. In the **SSON** field, enter the new SSON.

   The number must be between 128 to 254.
6. Press **Save**.

   Caution:

   Do not perform this procedure if you are using static addressing. Perform this procedure if you are using DHCP addressing and the DHCP option number is changed from the default number.

Related links

Accessing the Admin menu after log in on page 94

Accessing the View menu

About this task

Use this procedure to view the parameters associated with the administration procedures.

Procedure

1. Navigate to **Main Menu** > **Administration**.
2. In the **Access code** field, enter the Administration menu password, and press **Enter**.
3. Scroll to **View**, and press **Select**.

Related links

Accessing the Admin menu after log in on page 94

View field description

Setting	Description	Associated Configuration Parameter
Model	The model of the phone that is set by factory procedures.	MODEL
SW version	The version of the software.	
Backup SW version	The version of the software backup.	
Last update	Date of the last software update.	
Button modules	The model, IP address, and current status of the button module.	
FIPS	The status of FIPS mode (Enabled/Disabled)	
Protocol	Signaling protocol in effect, such as SIP.	
Group	The group identifier to download during start-up a specific configuration set for a dedicated user group.	GROUP
Ethernet MAC	MAC address of the phone.	
Serial number	The serial number of the phone.	
SIP proxy	The SIP proxy server to which the phone registered successfully.	SIPPROXYSRVR_IN_ USE

Table continues…

Setting	Description	Associated Configuration Parameter
Gateway	The address of the gateway.	
Gateway(V6)	The address of the IPv6 gateway.	
HTTPS server	The list of IP or FQDN addresses of TLS servers for HTTPS file download, settings file or language files, during startup.	TLSSRVR
HTTPS port	The port used for HTTPS file downloads from non-Avaya servers.	TLSPORT
HTTPS dir	The path name to prepend to all file names used in HTTPS GET operations during startup.	TLSDIR
HTTP server	The list of IP or FQDN addresses of HTTP servers for HTTP file download, settings file or language files, during startup.	HTTPSRVR
HTTP port	The TCP port used for HTTP file downloads from non-Avaya servers.	HTTPPORT
HTTP dir	The path name to prepend to all file names used in HTTP and HTTPS GET operations during startup.	HTTPDIR
DNS server	The IP address of the DNS server that the phone accessed before successfully.	DNSSRVR_IN_USE
SNTP server	The list of addresses of SNTP servers.	SNTPSRVR
STUN server	On the Avaya J129 IP Phone, displays the address of the STUN server. If the STUN server is not configured, or the resolution through the DNS server has failed, the `0.0.0.0` value is displayed. On the Avaya J139 IP Phone, Avaya J169/J179 IP Phones, and Avaya J189 IP Phone and press **Select** to view more details.	STUN_SERVER_ADDRESS
Product ID	The device ID of the phone.	
Device type	The default device type of the phone.	

Table continues…

Setting	Description	Associated Configuration Parameter
Server type	The default server type of the phone.	

Viewing the STUN server details

The STUN server menu contains the following information:

Field name	Description
Status	The current status of the STUN server. The possible statuses are: • **Active**: displayed in the following cases: - The STUN server is configured as an IP address. - The STUN server is configured as a Fully Qualified Domain Name (FQDN), and it can be resolved through the DNS server. • **Failed**: displayed when the STUN server is configured, but the resolution through the DNS server has failed. The possible reason might be that the DNS server is not available or the FQDN is incorrect. • **Not configured**: displayed when the STUN server is not configured.
Address	The IP address of the STUN server. For example, `10.10.10.1`. If the STUN server is not configured, or the resolution has failed, the value of `0.0.0.0` is displayed.
Port	The port the STUN server uses. For example, `3478`. If the STUN server is not configured, or the resolution has failed, the value is null (“0”).
Protocol	The protocol the STUN server uses. The possible values are: • **UDP**: displayed when the STUN server is configured, and the resolution through the DNS server is successful. • **Unknown**: displayed when the STUN server is not configured, or the resolution through the DNS server has failed.

Checking the phone update status

About this task

You can see the current status of the phone update information using the following procedure.

Procedure

1. Press **Main Menu** > **Administration**.
2. In the **Access code** field, enter the admin menu password and press **Enter**.
3. Scroll to **Update info** and press **Select**.

4. Scroll to **Status** and press **Select**.
5. The Status screen displays the following:
   - **Last update**: Displays the date and time of the last update of the phone.
   - **Next update**: Displays the date and time of the next update of the phone.
   - **Last upgrade**: Displays the date and time of the last firmware upgrade of the phone.

Related links

Accessing the Admin menu after log in on page 94

Checking the phone update policy

About this task

You can see the current policy of the phone update information using the following procedure.

Procedure

1. Press **Main Menu** > **Administration**.
2. In the **Access code** field, enter the admin menu password and press **Enter**.
3. Scroll to **Update info** and press **Select**.
4. Scroll to **Policy** and press **Select**.
5. The Policy screen displays the following:
   - **Automatic update policy**: Displays the current policy for the phone update.
   - **Update time of day**: Displays the current time slot for the phone update.
   - **Prompt on upgrade**: Displays the current setting for the user prompt on the phone screen before the phone upgrade.

Related links

Accessing the Admin menu after log in on page 94

IEEE 802.1X overview

The IEEE 802.1X standard provides specifications for secure layer 2 network access. Phones implement 802.1X supplicant in unicast and multicast modes and pass-through mode and proxy logoff for the attached device on the PC port.

When 802.1X is enabled, the phone ignores any incoming LLDP packets until the 802.1X authentication is completed or there is a time-out. The LLDP packets are processed after one of the following:

- 802.1X authentication completes successfully.
- 802.1X authentication fails.

- The phone does not receive a response from the switch on any 802.1X request for 90 seconds.

Note:

If the phone is in force-auth mode, there is an additional delay of 90 seconds during the phone boot-up.

Setting the 802.1x operational mode

About this task

The IEEE 802.1X standard provides specifications for secure layer 2 network access. Phones implement 802.1X supplicant in unicast and multicast modes and pass-through mode and proxy logoff for the attached device on the PC port. You can set the operational modes using this procedure.

Before you begin

- Make sure your RADIUS server and layer-2 network switch are configured correctly for 802.1x authentication.
- If you require EAP-TLS, pre-install the required identity certificates on the phone. For more information on certificates, see Identity Certificates.
- You can also enable 802.1x on the phone settings file, using the DOT1XSTAT parameter. If you use the settings file to configure 802.1x, make sure to align this change with a layer-2 switch and the RADIUS server. You can perform this step in a staging environment before deploying the phones for production use.

Warning:

Improper configuration of this feature can result in a site-wide outage of IP phones.

Procedure

1. Press **Main Menu** > **Administration**.
2. In the **Access code** field, enter the admin menu password.
3. Press **Enter**.
4. Select **802.1X**.

   The phone displays the following settings:

   - **Supplicant**
   - **Pass-thru mode**
5. Select the setting that you want to change.
6. Press **Toggle** soft key or the **Left** and **Right Arrow** keys to cycle through the following settings:
   - For the 802.1x Supplicant:
     - **Disabled**: 802.1x Supplicant is disabled.
     - **Unicast**: 802.1x Supplicant is enabled and works in unicast mode.

- **Multicast**: Supplicant is enabled and works in multicast mode.

• For the Pass-thru mode:

- **Enabled**: 802.1x packets from the PC port are forwarded to and from the layer-2 switch connected with the LAN interface of the phone.
- **Enabled logoff**: 802.1x packets from the PC port are forwarded to and from the layer-2 switch connected with the phone's LAN interface. The phone sends an EAP-Logoff when PC is disconnected.
- **Disabled**: 802.1x forwarding is disabled between PC port and the network switch. Do not select this option is PC is authenticated over 802.1x

7. Press **Save**.

   When you change the 802.1X data, the phone restarts after you exit the administration menu.

Related links

Accessing the Admin menu after log in on page 94
Identity certificates on page 351

Updating phone settings and firmware

About this task

Use this procedure to apply new settings from the file server or, if available, upgrade the phone firmware to a new version.

Procedure

1. Press **Main Menu** > **Administration**.
2. In the **Access code** field, enter the Administration menu password.
3. Press **Enter**.
4. Scroll to **Get updates**, and press **Select**.

   The phone displays the `Update may require a phone reboot` notification.

5. To apply the new settings or upgrade the phone to a new firmware version, press **Update**.

   If the file server contains the new settings which do not require a phone reboot, the Administration menu reappears. If the new settings require a reboot or a new firmware version is available, the phone reboots.

6. To exit the menu without applying the updates, press **Cancel**.

Related links

Accessing the Admin menu after log in on page 94

Resetting system values

About this task

Use this procedure to reset all system initialization values to the application software default values.

Caution:

This procedure erases all static information, without any possibility of recovering the data.

Procedure

1. Press **Admin menu** > **Administration**.
2. In the **Access code** field, enter the admin menu password.
3. Press **Enter**.
4. Select **Reset to defaults**.
5. Press **Reset** when the phone prompts for confirmation.

   The phone resets from the beginning of registration, which might take a few minutes. The phone resets all settings to the defaults except user data stored remotely.

   After reset, the phone displays the Log In screen.

   Note:

   To reset the phone default value when phone and web admin passwords are lost, press the key in the sequence of ‘Mute button’ ‘<phone mac address>’ ‘ #’. In the MAC address, ‘2’ is mapped to a, b, c and ‘3’ is mapped to d, e, f.

   For example, if the phone MAC address is A0:09:ED:05:80:51, the key sequence is ‘Mute 200933058051 #’.

   This applies to the phones in an Open SIP environment only.

Note:

Avaya J100 Series IP Phones parameters stored for a particular user are not reflected in other phones. For example, it is not reflected in 9600 Series IP Deskphones, even if the SIP user is the same.

Related links

Accessing the Admin menu after log in on page 94

Configuring the phone using the web interface

To remotely access the phone configuration, you can use the web interface of the phone. You can use the Administration menu of the phone or the `46xxsettings.txt` file to enable access to the web interface.

Warning:

For security reasons, you must disable the access to the web interface when you are not using it.

From the phone web interface, you can view the status of the configurations, configure the parameters, and reset the values to default. The following are the tabs on the web interface of Avaya J100 Series IP Phones:

- Status
- Network
- IP Configuration
- QoS
- NAT
- Web Server
- SIP
- Settings
- Date & Time
- Management
- Password
- Debugging
- Certificates
- Environment Settings
- Background and Screen Saver
- Calendar
- Multicast Paging
- Key Configuration
- Softkey Sets
- Shared Line Configuration
- Restart
- Reset to Default

Note:

There are some parameters with an asterisk (*). If you configure these parameters and save, restart the phone after you log out of the web interface.

There are some parameters with two asterisk (**). If you configure these parameters and save, the phone restarts immediately.

The phone web interface displays a globe icon against the parameter last modified from the web interface.

Enabling access to web interface of the phone

Administrators can enable access to the web interface of the phone through one of the following methods:

- By using the phone Administration menu.
- By setting the required parameter in the `46xxsettings.txt` file.

Enabling access to the web interface through the Administration menu of the phone

About this task

On the web interface of the phone, you can:

- Configure the parameters of the phone.
- View the status of the configurations.

The web interface access is active by default. Use this procedure for subsequent enabling.

Procedure

1. On the phone, press **Main menu**.
2. Scroll to **Administration**, and press **Select**.
3. In the **Access code** field, enter the administration password.

   The default access code is `27238`.
4. Press **Enter**.
5. Scroll to **Web server**, and press **Select**.
6. Scroll to **Web on HTTP**, and press **Toggle** to **Yes**.
7. Press one of the following:
   - **Save**
   - **OK**

Related links

Enabling Access to the Web interface

Web interface access through the settings file

Use the `46xxsettings.txt` file to set the following parameter to enable or disable access to the web interface:

Parameter	Default value	Description
ENABLE_WEBSERVER	1	Specifies whether the HTTP or HTTPS web server is enabled or disabled. The options are: • 0: Disable • 1: Enable

Viewing IP address of the phone

About this task

Use this procedure to obtain the IP address of the phone to log in to the web interface.

Procedure

1. On the phone, press **Main Menu**.
2. Scroll to **Administration**, and press **Select**.
3. In the **Access code** field, enter the administration password.

   The default access code is `27238`.
4. Press **Enter**.
5. Scroll to **IP Configuration**, and press **Select**.
6. Scroll to **Ethernet IPv4**, and press **Select**.
7. Scroll to **Phone**.

   The IP address is displayed next to the **Phone**.

Related links

Setting Up the Avaya J179 IP Phone Web interface

Logging in to the phone web interface

About this task

You can log-in to the phone web interface to do the following:

- Configure or edit the configuration of the phone.
- View the phone configuration.

Note:

When you log-in for the first time, you must change the default password and log in again with the new password.

Procedure

1. In your browser, enter the IP address of the phone and press **Enter**.

   The login page displays.

2. Enter the following:

   - In the **Username** field: The user name is always `admin`.
   - In the **Password** field: The default password is `27238` for the first time log in, you are forced to define a new password. For subsequent login enter the password you set.

3. Click **Login**.

   For the first time login, the phone web interface prompts you to change your default password.

   For subsequent login, you are logged into the phone web interface.

Related links

Setting Up the Avaya J179 IP Phone Web interface

Logging out of the phone web interface

Before you begin

Ensure you are logged into the phone web interface.

Procedure

Click **Logout** .

Password for the phone web interface

When you log into the phone web interface for the first time, you must change the password. Subsequently, anytime after the initial log in, you can change the password. The new password must comply with the following new rules:

- The length of the password must be between 8 to 31 characters.
- The password must have at least one numeral, one alphabet, and one special character.
- The password must have a maximum of four consecutive characters from the same character class.
- The password must have a maximum of two consecutive identical characters.

The allowed character class is numeric, upper case alphabet, lower case alphabet, and special character.

The allowed special characters are tilde (~), exclamation mark (!), at (@), pound (#), dollar ($), percent (%), carat (^), ampersand (&), asterisk (*), underscore(_), minus (-), plus (+), equal (=), back quote (`), pipe (|), back slash (\), parenthesis (()), braces ({}), brackets ([]), colon (:), semicolon (;), quote (“), single quote ('), lesser than (<), greater than (>), comma (,), period (.), question mark (?), forward slash (/).

Note:

The new web admin password rule applies for the phone software version 4.0.5 and later. You can continue using your old password until you reset it. When you upgrade the phone to a software version 4.0.5 or later, your old password remains valid until you reset it with a new password that complies with the new rules.

Changing the default phone web interface password

About this task

When you login to the phone web interface for the first time, it prompts you to change the default password.

Before you begin

Ensure that your new password complies with the new password rules.

Procedure

1. Log in to the web interface with your username and default password.
2. In the **Current Password** field, enter your current password.
3. In the **New Password** field, enter your new password
4. In the **Confirm Password** field, re-enter your new password.
5. Click **Update**.

Result

You are logged into the web interface of the phone.

Web interface screen layout

The web interface of the phone generally has the following layouts. Per your selection, each layout displays the corresponding details.

- The top bar displays the Avaya logo, phone model number, and Logout option.
- The sidebar on the left side of the screen, displays a list of tabs for selection.
- The center layout on the screen displays all the parameters and the corresponding user input field for the tab selected.
- The Expand All (+) or the Collapse All (-) icon on the top of the center layout and on the section header is for expanding or collapsing the sections in the center layout.

- The top section on the right side of the screen displays the Parameter Help. This section generally displays the parameter- description, type, the default value, and corresponding name in the settings file for the selected parameter.
- The section below the Parameter Help section displays the available sources for configuring the selected parameter.
- There are buttons Save and Reset to Default at the bottom of the center layout.

Changing the phone web interface password

About this task

To change the password of the phone web interface anytime after the first login.

Before you begin

Ensure that your new password complies with the new rules.

Procedure

1. Log in to the web interface with your username and current password.
2. In the navigation pane, click **Password**.
3. In the **Web Admin Password** section, do the following:
   a. In the **Current Password** field, enter your current password.
   b. In the **New Password** field, enter your new password.
   c. In the **Confirm Password** field, re-enter your new password.
   d. Click **Save**.

Viewing the status of the phone configuration

About this task

In the web interface of the phone, the Status tab displays all the configurations of the phone. You can see the latest values of the configurations on the status tab.

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Status**.
3. You can view any of the following configurations:
   - System
   - Interfaces
   - IP Mode

- IP Parameters (Ethernet)
- IP Parameters (Wifi)
- Plug-and-Play Configuration
- Configuration Server Address
- SIP Account
- Avaya Spaces
- Quality of Service
- 802.1x parameters
- VLAN
- SSL
- Web Server
- USB Headset Info
- USB Flash Drive Info
- USB Keyboard Info

4. To view the latest configuration values on the screen, click **Refresh**.

Status field description

Name	Description
System	
Model	Specifies the model number of the phone.
Software Version	Specifies the version number of the software in the phone.
Backup Software Version	Specifies the version number of the backup software in the phone.
Protocol	Specifies the protocol value set in the phone.
Group	Specifies the group value set in the phone.
Active MAC Address	Specifies the MAC address of the phone.
Ethernet MAC Address	Specifies the MAC address of the Ethernet interface of the phone. This is the MAC address which is used to provision the device in the DES.
WiFi MAC Address	Specifies the MAC address of the Wi-Fi interface of the phone. This MAC address is populated only when Wi-Fi chip is installed in the phone.
Serial Number	Specifies the serial number of the phone.
Product ID	Specifies the product ID of the phone.

Table continues…

Name	Description
Device Type	Specifies the device type. Example: Avaya SIP or Open SIP
Server Mode	Specifies the server mode set in the phone.
Last Phone Firmware Update	Specifies the date and the time of the firmware upgrade.
Last settings Update	Specifies the date and the time when the settings or the firmware were last updated.
Next settings Update	Specifies the date and the time of the next update of the settings.
Interfaces	
Active Interface	Specifies the active interface of the phone.
Ethernet Status	Specifies the ethernet status of the phone.
PC Ethernet Status	Specifies the PC ethernet status of the phone.
IP Mode	
IP Mode	Specifies the IP Mode value set in the phone.
IP Parameters (Ethernet)	
IPv4 Address	Specifies the IPv4 address of the phone.
Subnet Mask	Specifies the subnet mask of the phone.
IPv4 Gateway	Specifies the IPv4 gateway value set in the phone.
IPv6 Address	Specifies the IPv6 address of the phone.
IPv6 Link Local Address	Specifies the IPv6 link local address of the phone.
IPv6 Gateway	Specifies the IPv6 gateway value set in the phone.
SLAAC Address	Specifies the SLAAC address of the phone.
IP Parameters (Wifi)	
IPv4 Address	Specifies the IPv4 address of the phone.
Subnet Mask	Specifies the subnet mask of the phone.
IPv4 Gateway	Specifies the IPv4 gateway value set in the phone.
Plug-and-Play Configuration	
PNP Enabled	Specifies whether the PNP configuration is enabled or disabled.
PNP Status	Specifies the PNP status.
Configuration Server Address	
HTTPS Server	Specifies the address of the HTTPS server.
HTTP Server	Specifies the address of the HTTP server.
DNS Server	Specifies the address DNS server.
Backup/Restore Server for User data	Specifies the address of the Backup/Restore server.

Table continues…

Name	Description
SIP Account	
Registration Status	Specifies whether the SIP account is registered or not.
SIP User ID	Specifies the SIP user ID.
SIP Domain	Specifies the SIP domain.
SIP Proxy Server	Specifies the details of the proxy server.
Avaya Spaces	
Status	Specifies the current status of the feature on the phone.
Authentication	Specifies the current authentication mode of the Avaya Spaces feature.
Quality of Service	
L2 Audio	Specifies the L2 audio value set in the phone.
L2 Signaling	Specifies the L2 signaling value set in the phone.
L3 Audio	Specifies the L3 audio value set in the phone.
L3 Signaling	Specifies the L3 signaling value set in the phone.
802.1x parameters	
Supplicant	Specifies whether the 802.1x Supplicant is enabled or disabled.
Pass-through	Specifies whether the 802.1x pass-through is enabled or disabled.
VLAN	
VLAN ID	Specifies the VLAN ID of the phone.
SSL	
SSL Library Version	Specifies the version of SSL library used by the phone.
Open SSH Version	Specifies the version of open SSH used by the phone.
Web Server	
Web On HTTP	Specifies whether Webserver is allowed on the HTTP server.
HTTP Port	Specifies the port on which Webserver can be accessed on HTTP.
HTTPS Port	Specifies the port on which Webserver can be accessed on HTTPS.
USB Headset Info Available in Avaya J189 IP Phone	
USB Headset Model	Specifies the Headset Model if a USB Headset is connected to the phone.

Table continues…

Name	Description
USB Headset Manufacturer	Specifies the USB Headset Manufacturer if a USB Headset is connected to the phone.
USB Headset Firmware version	Specifies the USB Headset Firmware version if a USB Headset is connected to the phone.
USB Headset Serial number	Specifies the USB Headset Serial number if a USB Headset is connected to the phone.
USB Flash Drive Info Available in Avaya J159 IP Phone, and Avaya J189 IP Phone	
Flash Drive Model	Specifies the Drive Model if a USB Flash Drive is connected to the phone.
Flash Drive Manufacturer	Specifies the Drive Manufacturer if a USB Flash Drive is connected to the phone.
Flash Drive Firmware version	Specifies the Drive Firmware version if a USB Flash Drive is connected to the phone.
Flash Drive Serial number	Specifies the Drive Serial number if a USB Flash Drive is connected to the phone.
USB Keyboard Info Available in Avaya J159 IP Phone, and Avaya J189 IP Phone	
Keyboard Model	Specifies the Keyboard Model if a USB Keyboard is connected to the phone.
Keyboard Manufacturer	Specifies the Keyboard Manufacturer if a USB Keyboard is connected to the phone.
Keyboard Firmware version	Specifies the Keyboard Firmware version if a USB Keyboard is connected to the phone.
Keyboard Serial number	Specifies the Keyboard Serial number if a USB Keyboard is connected to the phone.

Configuring network settings

About this task

You can configure the network related settings from this tab.

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Network**.
3. Configure the following areas:
   - Network Mode
   - 802.1x Authentication
   - VLAN

- LLDP
- Ethernet Interface
- Wifi Interface
- Advanced

4. Click one of the following:
   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.

Network settings field description

Name	Description
Network Mode	
Network Mode of Operation	Specifies the network mode used by the phone. The operations are: • **Ethernet only** • **Ethernet (preferred, but manual override allowed from Phone UI) (default)** • **Wi-Fi (preferred, but manual override allowed from Phone UI)**
802.1x Authentication	
Supplicant Operating Mode	Specifies the 802.1x supplicant operating mode. The valid values are: • **Disable(default)** • **Supplicant Enable, responds only to received unicast EAPOL messages.** • **Supplicant Enable, responds to received unicast and multicast EAPOL messages.**
802.1x Pass-through Operating Mode	Specifies the 802.1x pass-through operating mode. The valid values are: • **Without proxy logoff (Default)** • **With proxy logoff** • **Disable**

Table continues…

Name	Description
Authentication Method	Specifies the authentication method used by 802.1x. The valid values are: • **MD5 (Default)** • **TLS**
VLAN	
802.1Q	Specifies whether layer 2 frames generated by the telephone will have IEEE 802.1Q tags. The valid values are: • Auto (Default): frames will be tagged if the value of L2QVLAN is non-zero • **On: frames will always be tagged.** • **Off: frames will never be tagged.**
VLAN ID	Specifies the voice VLAN ID to be used by IP telephones. The valid values are 0 through 4094. The Default value is 0.
VLAN Test	Specifies the number of seconds that DHCP will be attempted with a non-zero VLAN ID before switching to a VLAN ID of zero or to untagged frames. The valid values are 0 through 999 seconds. The Default value is 60. seconds
VLAN Separation Mode	Specifies whether VLAN separation will be Enable by the built-in Ethernet switch while the telephone is tagging frames with a non-zero VLAN ID. The valid values are: • **Enable (Default)** • **Disable**
PC Port VLAN ID	Specifies the VLAN ID to be used by frames forwarded to and from the secondary (PHY2) Ethernet interface. The valid values are 0 through 4094. The default value is 0.

Table continues…

Name	Description
Tags to PC Ethernet Interface	Specifies whether or not tags will be removed from frames forwarded to the secondary (PC) Ethernet interface. The valid values are: • **Remove (Default)** • **Do not remove**
LLDP	
LLDP	Specifies whether LLDP is Enable. The valid values are: • **Enable only if LLDP frame is received. (Default)** • **Enable** • **Disable**
Ethernet Interface	
Ethernet	Specifies the speed and duplex settings for the Ethernet line interface. The valid values are: • **Auto-negotiate (Default)** • **10Mbps half-duplex** • **10Mbps full-duplex** • **100Mbps half-duplex** • **100Mbps full-duplex** • **1Gbps full-duplex if supported by hardware**
PC Ethernet	Specifies the speed and duplex settings for the secondary (PC) Ethernet interface. The valid values are: • **Disabled** • **Auto-negotiate (Default)** • **10Mbps half-duplex** • **10Mbps full-duplex** • **100Mbps half-duplex** • **100Mbps full-duplex** • **1Gbps full-duplex if supported by hardware**

Table continues…

Name	Description
PC Ethernet auto-MDIX	Specifies whether auto-MDIX is Enable on PHY2. The valid values are: • **Disable** • **Enable (Default)**
WiFi Interface	
WiFi Control	
WLAN Network Configuration Mode	Specifies the Wi-Fi network configuration mode. The options are: • **Automatic (default)** • **Manual**
WiFi Setting	
Country	Specifies the country code to define the Wi-Fi radio parameters permitted by the local regulatory domain. Value format: two-character country code. The default value is **US**.
Use of 802.11d	Configures the 802.11d specifications automatically to the local regulatory domain for the WLAN network. The options are: • **Disable (default)** • **Enable**
WLAN Active SSID	Displays active SSID when Wi-Fi is active. This is an internal parameter. Value format: a sting from 0 to 32 characters. The default value is null.
SSID	Specifies the SSID string of the Wi-Fi network. Value format: alphanumeric characters and special symbols. **Note:** The space character (ASCII 0x20) is not supported. The default value is null.

Table continues…

Name	Description
Security	Specifies the WLAN security standard for your Wi-Fi network. The options are: • **None (default)** • **WEP Security** • **WPA/WPA2 security (pre-shared key) security** • **WPA2 Enterprise security (802.1x auth.)**
WLAN Max Authentication Retires	Specifies the number of retries that will be attempted to establish a secure connection upon receiving authentication failures. The options are: • **0** • **1** • **2** • **3 (Default)** • **4**
WEP	
WEP Key Length	Specifies the passcode key length for WEP security. The options are: • **64 bit** • **128 bit (default)**
WEP Default Key	Specifies the default key in your Wi-Fi network. The options are: • **WEP Key 1 (default)** • **WEP Key 2** • **WEP Key 3** • **WEP Key 4**

Table continues…

Name	Description
WEP Key 1	Specifies the WEP key values in the Wi-Fi network. The valid value is up to 26 alphanumeric characters that can be the following: • **Blank** • **0 – 9** • **A – F** The value must include 10 hexadecimal digits for 64 bit keys and 26 hexadecimal digits for 128 bit keys. The default value is null.
WEP Key 2	Specifies the WEP key values for the Wi-Fi network. The valid value is up to 26 alphanumeric characters that can be the following: • **Blank** • **0 – 9** • **A – F** The value must include 10 hexadecimal digits for 64 bit keys and 26 hexadecimal digits for 128 bit keys. The default value is null.
WEP Key 3	Specifies the WEP key values for the Wi-Fi network. The valid value is up to 26 alphanumeric characters that can be the following: • **Blank** • **0 – 9** • **A – F** The value must include 10 hexadecimal digits for 64 bit keys and 26 hexadecimal digits for 128 bit keys. The default value is null.
WEP Key 4	Specifies the WEP key values for the Wi-Fi network. The valid value is up to 26 alphanumeric characters that can be the following: • **Blank** • **0 – 9** • **A – F** The value must include 10 hexadecimal digits for 64 bit keys and 26 hexadecimal digits for 128 bit keys. The default value is null.

Table continues…

Name	Description
WPA2 Enterprise (802.1x)	
EAP Authentication Method	Specifies the type of EAP authentication method. The options are: • **PEAP (default)** • **TLS**
EAP Phase 2 Authentication Method	Specifies the type of EAP Phase 2 authentication method. The options are: • **None (default)** • **MSCHAPV2**
Authentication Identity	Specifies the pre-configured Wi-Fi network 802.1x identity. The valid value is a string of up to 32 alphanumeric characters and special symbols. The default value is null. **Note:** The space character (ASCII 0x20) is not supported.
Password	Specifies the pre-configured Wi-Fi network password. The valid value is a string of 8 to 63 characters for WPA/WPA2PSK and of 1 to 32 characters for 802.1x EAP. The default value is null. Value format: alphanumeric characters and special symbols. **Note:** The space character (ASCII 0x20) is not supported.
Authentication Anonymous Identity	Specifies the pre-configured Wi-Fi network 802.1x anonymous identity. The valid value is a string of up to 32 alphanumeric characters and special symbols. The default value is blank. **Note:** The space character (ASCII 0x20) is not supported.
Advanced	

Table continues…

Name	Description
ICMP	
Destination Unreachable Message Control	Controls whether ICMP Destination Unreachable messages are generated. The valid values are: • **No** • **Limited Port Unreachable messages (Default)** • **Protocol and Port Unreachable messages**
Redirect Message Control	Controls whether received ICMP Redirect messages will be processed. The valid values are: • **No(Default)** • **Yes**
TCP	
Send TCP Keep Alive Message	Specifies whether or not the telephone sends TCP keep alive messages. The valid values are: • **Enable (Default)** • **Disable**
TCP Keep Alive Time	Specifies the wait time interval in seconds of the phone before sending out the TCP keep-alive message (TCP ACK message) to the far-end. Valid value is an integer from 10 to 3600. The default option is 60 seconds.
TCP Keep Alive Interval	Specifies the TCP keep-alive packet re-transmission interval. Valid value is an integer from 5 to 60. The default option is 10 seconds.
TLS	
Use TLS Version	Specifies the TLS versions used in the network. The options are: • **1.0 and 1.2 (Default)** • **Only 1.2**

Configuring IP settings

Procedure

1. Log in to the web interface.

2. In the navigation pane, click **IP Configuration**.
3. Configure the following areas:
   - IP Version
   - IPv4 Configuration (Ethernet)
   - IPv6 Configuration (Ethernet)
   - IPv4 Configuration (Wi-Fi)
   - Servers
4. Click one of the following:
   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.

Ethernet settings field descriptions

Name	Description
IP Version	
IP Mode	Specifies the IP mode. The options are: • **IPv4 only** • **Dual mode (Default)** • **IPv6 only**
Dual Mode Operation Preference	Specifies the preference of the operation mode. The options are: • **IPv4 (Default)** • **IPv6**
Extended Re-bind Time	Specifies the time in seconds for which you can continue to use the assigned IP address after the DHCP lease expires. The valid value is an integer from 0 to 999. The default value is 60 seconds.
IPv4 Configuration (Ethernet)	

Table continues…

Name	Description
Use DHCP	Specifies whether to enable/disable DHCP as a source in IPv4 network. The options are: • **Yes (Default)**: To assign the IPv4 address automatically to your phone. • **No**: To assign the IPv4 address manually to your phone. **Note:** To assign the IP address manually, you must also configure the **IP Address**, **Subnet Mask**, and **Gateway IP Address** fields manually.
Continue to use DHCP information after lease expiry	Specifies whether the DHCP information can be used after the lease expires. The options are: • **Yes (Default)**: To use the assigned IP address after the DHCP lease expires. • **No**: To stop using the assigned IP address after the DHCP lease expires.
IPv4 Address	Specifies the IP address of the phone. You can enter the IP address in this field. The valid value is an IP address in the dotted decimal name format. The maximum number of characters is 15.
Subnet Mask	Specifies the network mask address. To assign the network mask address manually to your phone, type the address in this field. The valid value is an IP address in the dotted decimal name format. The maximum number of characters is 15.
IPv4 Gateway	Specifies the IP address of the gateway. The valid value is an IP address in the dotted decimal name format. The maximum number of characters is 15.
IPv6 Configuration (Ethernet)	
DHCPv6 Client Status	Specifies whether DHCPv6 Client is enabled or disabled. The options are: • **DHCPv6 client enabled (Default)** • **DHCPv6 client disabled**
Use DHCPv6	Specifies whether to use DHCPv6 as a source in IPv6 network. The options are: • **Yes (Default)**: To assign the IPv4 address automatically to your phone. • **No**: To assign the IPv4 address manually to your phone.

Table continues…

Name	Description
Continue to use DHCPv6 information after lease expiry	Specifies whether the DHCPv6 will comply with the IETF RFC 8415 standard and immediately stop using an IPv6 address if the address valid lifetime expires. The options are: • **Yes (Default)** • **No**
IPv6 Address	Specifies the IPv6 address of the phone. Value format: eight groups of four hexadecimal digits. The default value is null.
IPv6 Link Local Address	Specifies the link local address. Value format: eight groups of four hexadecimal digits. The default value is null.
IPv6 Gateway	Specifies the IP address of the gateway. Value format: eight groups of four hexadecimal digits. The default value is null.
Use SLAAC	Specifies whether to use Stateless Auto-Configuration. The options are: • **Yes (Default)** • **No**
Privacy SLAAC Mode	Specifies the preference for Privacy Extensions in SLAAC. The options are: • **Disabled, stable address generated from MAC** • **Stable private address (Default)** • **Temporary address**
SLAAC Addresses	SLAAC (stateless auto configuration) IPv6 addresses. Value format: eight groups of four hexadecimal digits. The default value is null.
IPv4 Configuration (Wi-Fi)	

Table continues…

Name	Description
Use DHCP	Specifies whether to enable/disable DHCP on WiFi network. The options are: • **Yes (Default)**: To assign the IPv4 address automatically to your phone. • **No**: To assign the IPv4 address manually to your phone. **Note:** To assign the IP address manually, you must also configure the **IP Address**, **Subnet Mask**, and **Gateway IP Address** fields manually.
IP Address	Specifies the IP address of the phone. The valid value is an IP address in the dotted decimal name format. The maximum number of characters is 15.
Subnet Mask	Specifies Subnet mask for WiFi. The valid value is an IP address in the dotted decimal name format. The maximum number of characters is 15.
Gateway IP Address	Specifies the WiFi gateway IP address. The valid value is an IP address in the dotted decimal name format. The maximum number of characters is 15.
Servers	
HTTPS Provisioning Server	
HTTPS Server Address	Specifies the IP address of the HTTPS provisioning file server. The valid value is the IP address in the dotted decimal name format, DNS name format or colon-hex. The default value is 0.0.0.0.
HTTPS Server Directory Path	Specifies the path to the configurations and data files in HTTPS GET operations during device bootup. This path is relative to the root of the HTTPS file server, to the directory in which the device configuration and data files are stored. If $MACADDR and/or $MODEL4 and/or $SERIALNO macro is present in the configured path then such macro is replaced with its actual value. The valid value is a string of up to 127 ASCII characters without spaces. This field is empty by default.
HTTPS Port	Specifies the HTTPS port address. The valid value is an integer from 0 to 65535. The default value is 443.
HTTP Provisioning Server	

Table continues…

Name	Description
HTTP Server Address	Specifies the IP address of the provisioning file server. The valid value is the IP address in the dotted decimal name format, DNS name format, or colon-hex. The default value is 0.0.0.0.
HTTP Server Directory Path	Specifies the path to the configurations and data files in HTTP and HTTPS GET operations during device bootup. This path is relative to the root of the HTTPS file server, to the directory in which the device configuration and data files are stored. If $MACADDR and/or $MODEL4 and/or $SERIALNO macro is present in the configured path then such macro is replaced with its actual value. The valid value is a string of up to 127 ASCII characters without spaces. This field is empty by default.
HTTP Port	Specifies the HTTP port address. The valid value is an integer from 0 to 65535. The default port number is 80.
Authentication Credentials to Provisioning Server	
User Name	Specifies the username for the HTTP Provisioning Server authentication. The default value is null.
User Password	Specifies the password for the HTTP Provisioning Server authentication. The default value is null.
DNS	
DNS Server	Specifies the DNS server address. Valid value is IP addresses in dotted-decimal format, separated by commas without any intervening spaces. The default value is null. You can add up to 16 DNS servers.
DNS Domain	Specifies the domain name of the DNS server. Valid value must be in the DNS name format. The default value is null.
SNTP	
SNTP Server	Specifies a list of the SNTP servers. The valid value is a string. The default value is 0.avaya.pool.ntp.org,1.avaya.pool.ntp.org,2.avaya.pool.ntp.org,3.avaya.pool.ntp.org

Table continues…

Name	Description
SNTP Sync Interval	Specifies the time interval in minutes at which the phone will attempt to synchronize its time with configured NTP servers. The valid value ranges is 60 through 2880 minutes. The default value is 1440 minutes.
GMT Offset	Specifies the time offset from GMT in hours and minutes. The valid value is a string. The default value is 0:00.

Related links

SNTP server configuration on page 47

Configuring QoS settings

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **QoS**.
3. Configure the following areas:
   - Ethernet QoS
   - WiFi QoS
4. Click one of the following:
   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.

QoS field descriptions

Name	Description
Ethernet QoS	
802.1P	
Audio Priority (Layer 2)	Specifies the Layer 2 priority value for audio frames generated by the phone. The valid value is an integer from 0 to 7. The default value is 6.
Signaling Priority (Layer 2)	Specifies the Layer 2 priority value for signaling frames generated by the phone. The valid value is an integer from 0 to 7. The default value is 6.

Table continues…

Name	Description
DiffServe	
Audio Priority (Layer 3)	Specifies the layer 3 Differentiated Services (DiffServ) code point for audio frames generated by the phone. The valid value is an integer from 0 to 63. The default value is 46.
Signaling Priority (Layer 3)	Specifies the layer 3 Differentiated Services (DiffServ) code point for signaling frames generated by the phone. The valid value is an integer from 0 to 63. The default value is 34.
WiFi QoS	
802.1P	
Audio Priority (Layer 2)	Specifies the Layer 2 priority value for audio frames generated by the phone when on WiFi. The valid value is an integer from 0 to 7. The default value is 6.
Signaling Priority (Layer 2)	Specifies the Layer 2 priority value for signaling frames generated by the phone when on WiFi. The valid value is an integer from 0 to 7. The default value is 6.
DiffServe	
Audio Priority (Layer 3)	Specifies the layer 3 Differentiated Services (DiffServ) code point for audio frames generated by the phone when on WiFi. The valid value is an integer from 0 to 63. The default value is 46.
Signaling Priority (Layer 3)	Specifies the layer 3 Differentiated Services (DiffServ) code point for signaling frames generated by the phone when on WiFi. The valid value is an integer from 0 to 63. The default value is 34.

Configuring NAT and STUN settings

About this task

Configure the NAT and STUN parameters for the phone to discover its public IP address and ports for SIP signaling, RTP, and RTCP. The phone's active private ports send periodic traffic, or keep-alive, to refresh the NAT bindings so that the NAT does not terminate them due to inactivity.

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **NAT**.
3. Configure the following areas:
   - NAT
   - STUN
4. Click one of the following:
   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.

NAT field descriptions

Name	Description
NAT	
Signaling keep-alive	Specifies whether the telephone sends keep-alive signals to refresh NAT bindings for the phone's private signaling IP address and port. The options are: • **Enable (default)**: Keep-alive messages are sent. • **Disable**: Keep-alive messages are not sent.
Signaling Keep Alive Interval	Specifies the interval, in seconds, between keep-alive signals used to refresh NAT bindings for the phone signaling IP address and port. Valid values: • None: The phone will use the default value. • 15 – 900: The phone will use this value as the keep-alive interval for every SIP registration and dialog. The default value is 15.
STUN	

Table continues…

Name	Description

STUN server	Specifies the STUN server address. If STUN server is not configured, other STUN settings listed after this parameter is ignored.
	The valid value is an IPv4 address in a dotted decimal format or a FQDN.
	For example,
	`SET STUN_SERVER_ADDRESS 192.168.161.54`
	or
	`SET STUN_SERVER_ADDRESS domain.com`

UDP initial timeout	Specifies the initial timeout, in milliseconds, to wait for a Response to a STUN Request sent over UDP. Valid values are positive integers from 500 (0,5 sec) to 3000 (3 sec). The default value is 500.
UDP max transmissions	Specifies the number of times the phone will transmit a STUN Request until a Response is received, after which the Request will be treated as failed. Valid values are positive integers from 1 to 7. The default value is 7.
UDP max transmissions for media	Specifies the number of times the phone transmits a STUN Request to get NAT bindings for the phone's RTP or RTCP IP address and ports. Valid values are 1 through 4. The default value is 3.

Configuring Web Server settings

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Web Server**.
3. Configure the following areas:
   - Web Server
   - Certificates
   - Web UI Layout
4. Click one of the following:
   - **Save**: To save the configuration changes.

- **Reset to Default**: To revert to the default values.

Web server field descriptions

Name	Description
Web Server	
Web Server On HTTP	Specifies whether HTTP access to the web interface is Enable or disabled. The options are: • **Yes (default)** • **No**
HTTP Listen Port	Specifies the port number of the web server when the web interface is accessed using HTTP. The valid value is an integer from 80 to 65535. The default port number is 80.
HTTPS Listen Port	Specifies the port number of the web server when the web interface is accessed using HTTPS. The valid value range is from 443 to 65535. The default port number is 443. The valid value is an integer from 443 to 65535.
Use certificate for Web Server	Specifies which server certificate will be used when the web interface is accessed using HTTPS. The options are: • **Factory Certificate (default)** • **Custom Certificate**
HSTS	Specifies whether the phone sends the HTTP Strict Transport Security (HSTS) header in the HTTP response. **Note:** If you enable this value, the phone sends the header only when the web UI is accessed over the HTTPS. The options are: • **Disabled (default)** • **Enabled**
Certificates	
Available Webserver Certificate	Specifies the trust certificates used as trust points for TLS connections. The valid value must be in `.pem` or `.p12` formats.

Table continues…

Name	Description
Upload Custom Webserver Certificate	Specifies the custom certificates to be uploaded. You can also browse and upload the certificates from the local machine by clicking **Browse** > **Import**
Password for Custom Webserver Certificate	Specifies the password to decrypt the uploaded certificate.
Web UI Layout	
Collapsible Sections for Web Interface	Specifies if the collapsible subsections on the WEB interface pages are enabled or disabled. The valid value is an integer from 0 to 63. The default value is 46. The valid values are: • Enabled (Default) • Disabled

Configuring SIP settings

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **SIP**.
3. Configure the following areas:
   - SIP Account
   - XSI
   - Busy Lamp Field (BLF)
   - SIP Global Settings
   - Codecs and DTMF
   - Codec Priority
   - RTP
   - SRTP
   - Voice Quality Monitoring
   - Timers and Count
   - Local Port
   - Miscellaneous
4. Click one of the following:
   - **Save**: To save the configuration changes.

- **Reset to Default**: To revert to the default values.

SIP settings field descriptions

Name	Description
SIP Account	
Registration Status	Displays the SIP account status. The field is automatically populated. The status can be the following: • Not Configured • Not Registered • Registered
Display Name	Specifies Caller ID, displayed for the remote party instead of a phone number or an extension number. Valid value is a text string of non-ASCI symbols.
Line/Port	User ID to log in to the phone. The valid value is a string. 20 characters (Blank, 0-9, A-Z, a-z, space and the following: * . , @ _ ! ' - +). The 'SIP Domain' and 'SIP Proxy server' must be configured to enable this field for configuration. The default value is null.
SIP User ID	Specifies the SIP user ID used to log in to the phone. You can also type the SIP user ID, which is a combination of the following values: • Upper and lower case characters. • Numbers from 0 to 9. • Spaces. • Special characters. The allowed characters are the following: . , : ; “” ‘’ / () {} [] ` ~ * _ ! ? + - ^ # = <> | & $ — The default value is empty.
Authentication User ID	Specifies the authentication ID. You can also type the authentication user ID in this field if authentication is enabled on the SIP server. The authentication user ID is a combination of the following values: • Upper and lower case characters. • Numbers from 0 to 9. • Spaces. • Special characters. The allowed characters are the following: . , : ; “” ‘’ / () {} [] ` ~ * _ ! ? + - ^ # = <> | & $ —

Table continues…

Name	Description
Authentication Password	Specifies the authentication password. You can also type the password in this field if authentication is enabled on the SIP server. **Note:** The password can contain maximum 31 ASCII characters. The default value is empty.
XSI Available only in BroadSoft environment.	
XSI State	Specifies the status of XSI. The values are: • Initializing • Success • Failure
XSI URL	Specifies the FQDN or the IP address, HTTP or HTTPS mode and the port of the XSP server. The valid value is a string of 0 to 255 ASCII characters.
XSI Event Channel Duration	Specifies the time duration in minutes for XSI event channel. The phone will ask 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 valid value is an integer from 60 to 1440. The default value is 60 minutes.
XSI Event Channel HeartBeat	Specifies the time interval in seconds to send heartbeat messages over Comet HTTP connection to XSP server of BroadWorks. The valid value is an integer from 1 to 999. The default value is 15 seconds.
XSI User Id	Specifies the BroadSoft user ID which the phone must use for XSI authentication. BroadSoft user Id is the SIP user Id excluding at (@) and domain. The valid value is a string of 0 to 255 ASCII characters.
XSI Web Password	Specifies the BroadSoft's web portal password which the phone must use for XSI web authentication. If the value is null, SIP authentication method is used.
Busy Lamp Field (BLF)	

Table continues…

Name	Description
BLF list URI	Specifies a unique name for the list of BLF users to monitor on the phone. The valid value is a string of up to 255 ASCII characters without any intervening spaces which can be entered in either of the following formats: • `sip:[list name]@[domain]` • `<list name>` The default value is empty. **Note:** Restart the phone to apply the changes to this settings.
BLF list Preferred Start Location	Specifies the starting location from which the detected BLFs is placed on the phone home screen. The valid value ranges between 0 to 96. The default value is 0. Where, the BLF is placed depending on the number of connected button modules. Starting location is 1 if no BLFs are detected from **BLF list URI**. Starting location is 25 if there are no button modules connected. For value 1-96, the BLF is placed at the specified location.
Force BLF list Line key Location	Specifies that the BLF line key cannot be moved or modified on the phone home screen. The Forced properties are detected from **BLF list URI**. The options are: • **Unforced** • **Forced (User cannot move the BLF list line keys) (Default)**
Allow User to Change BLF List (this field is available only in the BroadSoft environment)	Specifies the control to provide the user permissions to add and remove BLF monitored users from the phone. The values are: • **User is allowed to add or delete BLF monitored users** • **User is allowed to add BLF monitored users** • **User is allowed to delete BLF monitored users** • **User is allowed to add and delete BLF monitored users (default)**
SIP Global Settings	
SIP Domain	Specifies the SIP domain used for SIP registration. The valid value is a string of 0 to 255 ASCII characters.

Table continues…

Name	Description
Enable PPM as source of Proxy Server	Specifies whether PPM is used as a source of SIP proxy server information. **Note:** This is an Avaya Aura® setting which is ignored in an Open SIP environment. The options are: • **Yes (default)** • **No**
UDP Transport	Specifies whether UDP transport is allowed. The options are: • **Do Not Allow (default)** • **Allow**
Proxy Policy	Specifies whether SIP proxy servers are read-only or can be edited. The options are: • **Manual (Use Phone Admin Menu or WEB to configure)**: To configure SIP proxy server manually by using the phone or the web interface. • **Automatic (Can be set from DHCP, LLDP, Settings File, PPM) (default)**: To use the SIP proxy server settings received from the `46xxsettings.txt` file .
SIP Proxy Server	Specifies a list of SIP controller designators. You need to set the Proxy Policy value to Manual, to change the value of SIP Proxy Server. The syntax is Server[:Port;transport=Method],[Server:Port[Port];[transport=Method]] Server can be an IP address or FQDN. Port is the SIP port used by the server. (default 5061 if Method is TLS, 5060 if Method is UDP or TCP). Method is the transport connectivity method [TLS, TCP, UDP]. default value for Method is TLS. When FQDN is defined the phone performs DNS SRV. The Default value is null.
SIP Proxy Server (Automatic)	Specifies the SIP proxy server settings as received from the `46xxsettings.txt` file .
Register to Proxy Server	Specifies whether the phone registers simultaneously to a proxy server. The options are: • **Simultaneous (default)** • **Alternate**

Table continues…

Name	Description
Number of proxy server to register simultaneously	Specifies the number of SIP proxy controllers that the phone can register simultaneously. The options are: • **1** • **2** • **3** • **4** • **5 (Default)**
Number of Line Appearances	Specifies the number of line appearances that the phone will display. For each displayed line appearance there is a specific line appearance index. The options range from **1** to **10** line appearances. The default value is **3**.
Authentication User-ID Field	Controls the display of the User ID input field on the phone Login Screen, and Authentication User ID on the Web UI SIP Account tab. The options are: • **Enabled** • **Disabled (default)**
Registration Interval	Specifies the time interval in seconds between two registrations to the SIP proxy. The valid value is an integer from 30 to 86,400. The default value is 900 seconds.
Un-registration Wait Timer (seconds)	Specifies the time in seconds during which the phone waits before terminating all SIP dialog and SIP registrations. The valid value is an integer from 4 to 3,600. The default value is 32 seconds.
Registration Wait Timer (seconds)	Specifies the time in seconds during which the phone waits for a response message from registration. If no response message is received within this time, the phone tries to register again. The valid value is an integer from 4 to 3,600. The default value is 32 seconds.
Signaling IP Preference	This parameter is used by SIP signaling only on a dual mode phone (phone with both IPv4 and IPv16 addresses configured) to select the preferred SIP controller IP addresses. The default value is **IPv4**.
Media IP Preference	Specifies the preference of SDP media group lines and the SDP answer/offer format when phone is in dual mode. The default value is **IPv4**.
Codecs and DTMF	

Table continues…

Name	Description
OPUS	Specifies whether the OPUS codec capability of the phone is enabled or disabled. The options are: • **Disabled** • **Enabled WIDEBAND_20K (default)** • **Enabled NARROWBAND_16K** • **Enabled NARROWBAND_12K**
G.722	Specifies whether the G.722 codec is enabled. The options are: • **Disable** • **Enable (default)**
G.726	Specifies whether the G.726 codec is enabled. The options are: • **Disable** • **Enable (default)**
G.729	Specifies whether the G.729A codec is enabled. The options are: • **Disable** • **Enable without Annex B support (default)** • **Enable with Annex B support**
G.711u law	Specifies whether the G.711u law codec is enabled. The options are: • **Disable** • **Enable (default)**
G.711a law	Specifies whether the G.711a law codec is enabled. The options are: • **Disable** • **Enable (default)**
Send DTMF	Specifies whether the phone sends DTMF tones in-band as regular audio, or out-of-band using RFC 2833 procedures. The options are: • **In-band** • **Out-of-band (default)**

Table continues…

Name	Description
OPUS Payload	Dynamically specifies the RTP payload type to be used for OPUS codec. The parameter is used when the media request is sent to the far-end in an INVITE or 200 OK when INVITE with no Session Description Protocol (SDP) is received. The valid value is an integer from 96 to 127. The default value is 116.
G.726 Payload	Specifies the RTP payload type to be used for the G.726 codec. The valid value is an integer from 96 to 127. The default value is 110.
DTMF Payload	Specifies the RTP payload type to be used for RFC 2833 signaling. The valid value is an integer from 96 to 127. The default value is 120.
Codec Priority	Specifies the preferred priority of codecs. To set the parameter see Assigning Codec Priority on page 155
RTP	
Play Tone till RTP	Specifies whether the locally generated ringback tone stops when SDP is received for an early media session, or whether it continues until RTP is actually received from the far-end party. The options are: • **Yes (default)** • **No**
Symmetric RTP	Specifies whether the phone must receive RTP if the UDP source port number is not same as the UDP destination port number. The options are: • **Disable** • **Enable (default)**
SRTP	

Table continues…

Name	Description
Media Encryption	Specifies the crypto suite and session parameters for media encryption. The options are: • **aescm128-hmac80** • **aescm128-hmac32** • **aescm128-hmac80-unauth** • **aescm128-hmac32-unauth** • **aescm128-hmac80-unenc** • **aescm128-hmac32-unenc** • **aescm128-hmac80-unenc-unauth** • **aescm128-hmac32-unenc-unauth** • **none (default)** • **aescm256-hmac80** • **aescm256-hmac32** **Note:** You should not use unauthenticated media encryption (SRTP) options.
Encrypt RTCP	Specifies whether RTCP packets are encrypted or not. The options are: • **Yes**: SRTCP is enabled. • **No (default)**: SRTCP is disabled.
Enforce "SIPS" URI for SRTP	Specifies whether a SIPS URI must be used for SRTP. The options are: • **Yes (default)**: Enforced • **No**: Not enforced.
SDP Negotiation Capability	Specifies the Session Description Protocol (SDP) negotiation capability. • **Yes (default)** • **No**
Voice Quality Monitoring	

Table continues…

Name	Description
RTCP_XR	Specifies whether and how VoIP Metrics Report Block as defined in RTP Control Protocol Extended Reports (RTCP XR) (RFC 3611) is sent. The options are: • **Disable**: RTCP XR is not sent to remote peers and to any voice monitoring servers. • **Enable for peers and voice monitoring servers**: RTCP XR is sent to remote peers and to any voice monitoring servers • **Enable for voice monitoring servers only**: RTCP XR is sent to RTCP monitoring server only.
RTCP Monitor Address	Specifies the IP or DNS address of the RTCP monitor. The valid value is a string of up to 255 ASCII characters. The default value is empty.
RTCP Monitor Port	Specifies the RTCP monitor port number. Valid value is an integer from 0 to 65535. The default value is 5005.
RTCP Monitoring Report Period	Specifies the time interval in seconds for sending out RTCP monitoring reports. Valid value is an integer from 5 to 30. The default value is 5 seconds.
RTCP Publish Address	Specifies the SIP URI target. Phone sends VQ-RTCPXR voice quality metric reports using this address in SIP PUBLISH message per RFC 6035. This parameter works independent of RTCP Monitoring settings. This address should not have sip scheme. The domain of the URI can be an IP address or a FQDN. The value ranges from 0 to 255 characters; the default value is null. A valid example: user@domain.com, an invalid example: sip:user@domain.com
Timers and Count	
SIP Timer T1	Specifies an estimate in milliseconds for the Round Trip Time (RTT). The valid value is an integer from 500 to 10,000. The default value is 500 milliseconds.
SIP Timer T2	Specifies the maximum retransmit interval in milliseconds for non-INVITE requests and INVITE responses. The valid value is an integer from 2,000 to 40,000. The default value is 4,000 milliseconds.
SIP Timer T4	Specifies the maximum duration in milliseconds for which a message remains in the network. The valid value is an integer from 2,500 to 60,000. The default value is 5,000 milliseconds.

Table continues…

Name	Description
INVITE Response Timeout	Specifies the maximum number of seconds that the phone waits for another response after receiving a SIP 100 Trying response. The valid value is an integer from 30 to 180. The default value is 60 seconds.
Failed Session Removal Timer	Specifies the time in seconds to automatically remove a failed call session. The valid value is an integer from 5 to 999. The default value is 30 seconds.
Outbound Subscription Duration Request	Specifies the outbound subscription request duration in seconds. The valid value is an integer from 60 to 31,536,000. For NetSapiens, the valid value range is 300 through 31,536,000. The default value is 86,400 seconds.
Controller Search Interval	Specifies the time in seconds that the phone waits to complete the maintenance check for monitored controllers. The valid value is an integer from 4 to 3,600. The default value is 16 seconds.
Active subscription wait time for "avaya-cm-feature-status"	Specifies the time in seconds that the phone waits to validate an active subscription when it subscribes to the avaya-cm-feature-status package. The valid value is an integer from 16 to 3,600. The default value is 32 seconds.
Remote Data Source initial retry time	Specifies the number of seconds that the phone waits for the first time before trying to contact the PPM server again after a failed attempt. Each subsequent retry is delayed by double the previous delay time. The valid value is an integer from 2 to 3600. The default value is 2 seconds.
Remote Data Source maximum retry time	Specifies the maximum delay interval in seconds after which the phone stops to contact the PPM server. The valid value is an integer from 2 to 3,600. The default value is 600 seconds.
Remote Data Source initial retry attempts	Specifies the number of attempts the PPM adaptor must try to download from PPM before it stops connecting to the PPM server. The valid value is an integer from 1 to 30. The default value is 15 attempts.
Local Port	
RTP Port (minimum)	Specifies the lower limit of a port range. The valid value is an integer from 1024 to 65,503. The default value is 2048.

Table continues…

Name	Description
RTP Port (range)	Specifies the port range to be used by the following connections: The valid value is an integer from 32 to 63487. The default value is 40.
SIP Signaling Port (minimum)	Specifies the lower limit of a port range to be used for SIP signaling. The valid value is an integer from 5062 to 65,503. The default value is 1024.
SIP Signaling Port (range)	Specifies the port range to be used for SIP signaling. The valid value is an integer from 32 to 64511. The default value is 64511.
Miscellaneous	
Conference Factory URI	Specifies the URI for network conferencing in Open SIP environments. The valid value is a string of up to 255 ASCII characters.
Subscribe Event Packages	Specifies a comma-separated list of event packages to subscribe to after registration. Allowed values are: • `reg` • `dialog` • `mwi` • `ccs` • `message-summary`, which is identical to `mwi` • `avaya-ccs-profile`, which is identical to `ccs` For the Open SIP environment, you can use `message-summary`.
Voice Mail Access Code	Specifies the number to access the voice mail in a non-Avaya environment.
100rel	Specifies whether the 100rel option tag is included in the SIP INVITE header field. The options are: • **Disable**: The tag is not included. • **Enable (default)**: The tag is included.
Validate Incoming messages	Specifies whether AOR received in Request-URI of an incoming call must be validated with the contact header published by phone during registration. The options are: • **Disable (default)** • **Enable**

Table continues…

Name	Description
'Privacy' header in Incoming message	Specifies whether AOR received in Request-URI of an incoming call must be private in the contact header published by the phone during registration. The options are: • **Display CallerID information (default)** • **Display 'Restricted'**
Validate host in SIP URI	Specifies whether to accept SIP URI with unrecognized host part in INVITE message. The valid options are: • **Enable (Default)**: do not accept the SIP URI with unrecognized host. • **Disable**: accept the SIP URI with unrecognized host.

Assigning Codec Priority

Procedure

1. Log in to the web interface
2. In the navigation pane, click **SIP**.
3. Scroll to **Codec Priority**.
4. Select the required Codecs from the list box **Default** and press the forward arrow (>>) button.

   The selected Codecs are displayed in the **Custom** list box.
5. Use the **Up** and **Down** button to set the priority.

   The priority sequence is from top to bottom. The Codec which is on the top of the list has the highest priority.

Configuring Settings

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Settings**.
3. Configure the following sections:
   - Language
   - Feature Access
   - Broadsoft Call Center, available only in BroadSoft server mode.
   - Broadsoft Flexible Seating and Hoteling, available only in BroadSoft server mode.
   - Feature Access Codes (FAC)

- Alerting on Calls
- Phone Menu Options
- Call Log
- Contacts
- LDAP contacts
- Emergency Call
- Phone Lock
- Audio
- Dialing
- Ringtones
- Show or Hide Ringtones on Phone User Menu
- Enhanced Local Dialing Rules
- Admin
- MLPP
- Guest Login
- Save Extension
- Bluetooth
- CCMS
- Brightness
- USB, available in Avaya J159 IP Phone, and Avaya J189 IP Phone
- Privacy
- Downloadable Directory
- Avaya Spaces
- Other

4. Click one of the following:
   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.

Related links

Call center agent and supervisor on page 282
Call disposition codes on page 283
Configuring Secure Mode on the Avaya J179 IP Phone

Settings field descriptions

Settings

Name	Description
Language	
Import Language File	Browse and import a language file from your local machine by clicking **Browse** > **Import**.
Language file to upload	Specifies the language files to be installed on the phone. Filenames can be full URL, relative pathname, or filename comma separated filenames ending with `.xml`. The default value is empty.
Phone Language	Specifies the language used in phone system. Value format: complete language file name from 0 to 32 characters, for example: `Korean.xml`. The default value is empty.
Feature Access	
Call Forward	Specifies the status of the Call Forwarding feature. The options are: • **Off (default)** • **Unconditional** • **Busy** • **Unconditional and Busy** • **No answer** • **Unconditional and No answer** • **Busy and No answer** • **Unconditional, No answer and Busy**
Number of Ring cycle before Call Forward	Specifies the number of ring cycles before the call is forwarded. The valid value is an integer from 0 to 20. The default number of ring cycles is 1.
Do Not Disturb	Specifies the status of the Do Not Disturb feature. The options are: • **Do Not Allow** • **Allow (default)**

Table continues…

Name	Description
DND Priority over Call Forward (Unconditional, Busy)	Specifies the priority between the Do Not Disturb and Call Forward (Unconditional/Busy) features when both are activated by the user. The options are: • **Yes** • **No (default)**
Auto Answer Support	Specifies the status of the Auto Answer feature. The options are: • **Do Not Allow (default)** • **Allow**
Mute on Auto Answer	Specifies muting when the Auto Answer feature is enabled. The options are: • **Yes (default)** • **No**
Auto-answer during a call	Specifies whether to auto-answer calls during an active call. The valid values are: • **No (Default)**: do not auto-answer when there is an active call. • **Yes**: auto-answer when there is an active call. The current call is put on hold.
Hold Reminder Timer	Specifies the time in seconds after which the phone plays the hold reminder tone. The valid value is an integer from 0 to 999. The default value is 0 seconds.
Hold Reminder Display	Specifies whether the called party name or number with the text hc [Return] is displayed on call appearance when the phone reminds the user about a held call. The options are: • **Disable** — The called party name or number is displayed on call appearance when the phone reminds the user about a held call. • **Enable (default)** — The called party name or number with the text hc [Return] is displayed on call appearance when the phone reminds the user about a held call.

Table continues…

Name	Description
Conference continues on host hangup	Specifies whether a conference call continues after the host hangs up. The options are: • **Yes** • **No (default)**
Shortcut action BLF	Specifies the shortcut action performed by activating the BLF line during an active call or, in case of Call Park, during an active or a held call. The options are: • **Call to BLF destination (default)** • **Transfer to BLF destination** • **Blind transfer to BLF destination** • **Conference to BLF destination** • **Park to BLF destination** Call park shortcut action is available only in the Broadworks environment.
Shortcut action Contact	Specifies the shortcut action performed by activating the Contact line during an active call or, in case of Call Park, during an active or a held call. The options are: • **Call to Contact destination (default)** • **Transfer to Contact destination** • **Blind transfer to Contact destination** • **Conference to Contact destination** • **Park to Contact destination** Call park shortcut action is available only in the Broadworks environment.

Table continues…

Name	Description
Shortcut action Autodial	Specifies the shortcut action performed by activating the Autodial line during an active call or, in case of Call Park, during an active or a held call. Using Autodial line keys as shortcuts is available only in the Broadworks environment. The options are: • **Call to Autodial destination (default)** • **Transfer to Autodial destination** • **Blind transfer to Autodial destination** • **Conference to Autodial destination** • **Park to Autodial destination** Call park shortcut action is available only in the Broadworks environment.
Call Decline policy	Specifies whether the user can decline the incoming call. You can enable and disable the feature using the following options: The options are: • **Disabled (Default)** • **486 method**: By selecting this value you enable the Call decline policy for the user. 486 method indicates that the call ringing location is not available to take the call. However, the ringing continues in other locations. • **603 method**: By selecting this value you enable the Call decline policy for the user. 603 method indicates that no location is available to take the call.
Shortcut action BLF Park	Specifies the way parking a call is performed when the Shared Parking line is activated during an ongoing call. The options are: • **Blind transfer to BLF Park destination (default)** • **Dial Park FAC + BLF Park destination**: this option might not be available in all the environments.

Table continues…

Name	Description
Call Park Dynamic and Page	Specifies whether the Park and Page feature is available to the user. This feature requires that the **CALL_PARK_DYNAMIC_FAC** code and **CALL_PARK_DYNAMIC_METHOD** are defined in order to park the call. The options are: • **Disable** • **Enable** If Call Park Dynamic and Page is disabled, Call Park Dynamic Method, Call Park Dynamic FAC, Call Page Extension FAC, Call Paging Group and Call Page Group FAC are grayed out. The default value is Disable.
Call Park Dynamic Method	Specifies the method to initiate the Park Dynamic feature. The options are: • **Blind transfer**: The active call is blind transferred to the **CALL_PARK_DYNAMIC_FAC** • **DTMF**: Provide the **CALL_PARK_DYNAMIC_FAC** digits into the active call. The default value is Blind transfer.
Call Paging Groups	Specifies a comma separated list of paging groups a user is allowed to call. PagingGroupLabel:PagingGroupAddress — PagingGroupLabel is a string describing the PagingGroupAddress. PagingGroupAddress is the address or number of the PagingGroupLabel. PagingGroupLabel can be of 32 unicode characters and PagingGroupAddress can be of 64 unicode alphanumeric characters, an extension, an address or sip uri.PagingGroupLabel and PagingGroupAddress can not contain: ;",=|<>/&. For example : TechSupport:34299,Sales:34277 The default value is null.

Table continues…

Name	Description
Prioritize incoming calls	Specifies if visual display of incoming alerts are to be sorted when there is more than one or if they should be displayed in the order they are received. Incoming alerts can include (in priority order): incoming calls, calls parked to the user's extension, incoming calls to a monitored BLF key, calls parked to a monitored BLF key. The options are: • **Disable**: sort the list of incoming alerts in the order they are received. • **Enable**: sort the list of incoming alerts by priority. The default value is null.
Keep current CA	Specifies whether the selected line on the phone screen will remain selected if the line is a call appearance with a call that is just ended. The call can be on a primary call appearance, a bridged call appearance or a shared call appearance. The options are: • **Disable**: select a higher priority call or reset to select the first line if the phone is idle. • **Enable**: keep the current line selection. The default value is null.
Phone screen mode	Specifies the default layout of the main phone screen. Also specifies if the user can change the layout or not. This option is available only in Open SIP environment. The options are: • Full-user adjustable • Half-user adjustable • Half-locked • Full-locked
Scrolling mode	Specifies the scrolling mode on the Phone and Feature screens. The options are: • **Line scrolling (Default)**: the user can navigate by using the phone Up and Down navigation keys to select the previous or next line is selected. User can use the left and right navigation keys to select another column in dual screen mode. • **Page scrolling**: the user can use the left and right navigation keys to switch between the previous and next page.

Table continues…

Name	Description
Ignore BLF line key	Specifies if Softkey1 action will not be performed when the user presses line key associated with a BLF line, this parameter is not applicable when the user presses a BLF key in a Conference/Transfer/Page Target or similar selection modes. The options are: • **Yes**: the softkey1 action is ignored • **No (Default)**: the softkey1 action is not ignored. Avaya J129 IP Phone does not support this.
Ignore line key	Specifies if the action of Softkey1 on the phone screen is performed or ignored when the user's call appearance is on an active call and the user presses the line key associated with the active call. The options are: • **Yes (Default)**: the softkey1 action is ignored • **No**: the softkey1 action is not ignored. Avaya J129 IP Phone does not support this.
Broadsoft Call Center	
Enabled	You can enable or disable the Broadsoft Call Center feature for the user of the phone.
Active	Specifies if the logged in user is assigned to at least one call center as an agent.
Unavailable codes	You can enter a list of reason codes which the agent can select when they are going to be unavailable. Example: Code=description, 1=coffee break, DND=Do Not Disturb
Disposition codes	You can enter a list of disposition codes which the agent can select when they categorise a call. Example: Call center ID:Code=Description, 1=Follow-up required, sales:2=New customer Disposition code does not support special characters.
Supervisors	You can add supervisors to the call centers, whom the agents can select when they have an emergency escalation. Example: Call center ID:Extension=Description, 6551=Supervisor1, sales:6552=Supervisor2, helpdesk:6553=Supervisor3
Enable Customer Originated Trace	You can enable or disable the Customer Originated Trace for the agents.

Table continues…

Name	Description
Automatic state change	Specifies if the phone should automatically set state Sign-In and Sign-Out on login and logout, respectively. The valid values are: • **No (Default)** • **Yes**
Feature Access Codes (FAC)	
Call Pickup	Specifies that when a BLF key is receiving an incoming call, the phone will provide the user a context sensitive Pickup soft key, if the Call Pickup FAC is defined. Call Pickup FAC can be used with Busy Lamp Field (BLF) feature keys. The default value is *97.
Call Pickup Barge In	Specifies that when a BLF key is on a active call, the phone will provide the user a context sensitive Barge In soft key, if the Call Pickup Barge In FAC is defined. Call Pickup Barge In FAC can be used with Busy Lamp Field (BLF) feature keys. The default value is *33.
Call Park	Specifies that a Call Park FAC can be used to park a call. If Call Park FAC is defined this FAC will be prepended to the dialstring when executing a Shortcut Action The default value is Null.
Call Park Dynamic	Specifies that a Call Park Dynamic FAC can be used to park a user's call where the server will dynamically assign the park location. Typically the user will then hear an announcement by the server where the call is parked The default value is Null.
Call Page Extension	Specifies that a Call Page Extension FAC is used to inform the server to perform a page to an extension The default value is Null.
Call Page Group	Specifies that a Call Page Group FAC specifies the feature access code that phone will prepend to a user selected Paging Group call. If the Call Page Group FAC is not defined then a user selected Paging Group address will be dialed directly The default value is Null.
Call UnPark	Specifies that a Call UnPark FAC can be used to retrieve a parked call. If Call Unpark FAC is defined this FAC will be prepended to dial string when pressing a busy BLF Park key. The default value is *88.

Table continues…

Name	Description
Escalation	Specifies that an Escalation FAC can be used by the phone to invoke Broadworks call center Escalate feature. The value specified by you is ignored if the phone receives another value from XSI. The default value is Null.
BLF Pickup Method	Specifies which method will be used to pickup the BLF call. The valid values are: • Invite with FAC in Request URI (Default) • Invite with Replaces header
Alerting on calls	
BLF Incoming call indication type	Specifies the type of indication for BLF incoming call. The valid values are: • **None**: no alerting. • **Audible**: only audio alerting. • **Visual**: only visual alerting. • **Both (Default)**: both audio and visual alerting. • **Force none**: forced no alerting. • **Force audible**: forced only audio alerting. • **Force visual**: forced only visual alerting. • **Force both** : forced both audio and visual alerting.
BLF Parked Call indication type	Specifies the type of indication for BLF Parked call indication. The valid values are: • **None**: no alerting. • **Audible (Default)**: only audio alerting. • **Visual**: only visual alerting. • **Both**: both audio and visual alerting. • **Force none**: forced no alerting. • **Force audible**: forced only audio alerting. • **Force visual**: forced only visual alerting. • **Force both** : forced both audio and visual alerting.

Table continues…

Name	Description
Beacon indication mode	Specifies the behavior of the beacon LED. Applies to both primary and shared lines. The valid values are: • **Immediate (Default)**: Beacon LED will flash immediately, when there is an incoming call and until it is answered. • **Delayed**: Beacon LED will flash after a delay per delayed ringing configuration, when there is an incoming call and until it is answered or ignored.
Phone Menu Options	
Settings	Specifies whether the Settings menu is displayed on the phone. The options are: • **Do Not Allow** • **Allow (default)**
Network Info Screen	Specifies whether the Network Information screen is displayed on the phone. The options are: • **Do Not Allow** • **Allow (default)**
SIP User Logout	Specifies whether the Logout feature is provided to the user. The options are: • **Do Not Allow** • **Allow (default)**
Show SSL Version	Specifies the version of the SSL certificate.
Network Configuration by User	Specifies whether the network configuration can be modified by the user. The options are: • **Do Not Allow to Modify** • **Allow to Modify (default)**
Call Log	
Call Log	Specifies whether to enable or disable the Call Log application on the phone. The options are: • **Do Not Allow** • **Allow (default)**

Table continues…

Name	Description
Redial Softkey	Specifies whether the **Redial** soft key is available. The options are: • **Do Not Allow** • **Allow (default)**
Redial in Phone Menu	Specifies whether phone redials the last number or displays the list of recently dialed numbers. The options are: • **Do Not Allow (default)** • **Allow**
Redial Softkey Options	Specifies whether to show a list or one number on the **Redial** soft key. The options are: • **List (Redial out of list)** • **One number (default)**
Default redial list mode	Specifies that if this parameter is set to Last number redial or Redial list, then it specifies default Redial button action. If this parameter is set to forced, then the Redial Softkey Options parameter will be ignored and the option to pick effect of redial button disappears from Phone UI user menu. The options are: • **Last number redial (Default)** • **Redial list** • **Last number redialed Forced** • **Redial list Forced**
Log answered elsewhere calls	Specifies the local call log behavior when an incoming call to the phone is answered elsewhere by another user or device. The options are: • **As missed call (Default)** • **As answered call** The default value is as missed call.
Contacts	

Table continues…

Name	Description
Local Contacts	Specifies whether to enable or disable the Contacts application on the phone. The options are: • **Do Not Allow** • **Allow (default)**
Contact Name Format	Specifies the format of the contact name to be displayed in the Contacts list. The options are: • **'Last Name' 'First Name' (default)** • **'First Name' 'Last Name'**
Contact Name display logic	Specifies how to match a dialed string on an incoming call with the users contacts. The options are: • **Match the number completely (default)** • **Match shorter number completely to the rightmost digits of longer number** • **Match at least 4 rightmost digits**
LDAP contacts	
Enable LDAP Search	Specifies whether the LDAP Directory feature is enabled on the phone. If LDAP Directory is enabled, users can select it as a contact search source. When LDAP is enabled, other contact search sources become disabled. The options are: • **Enabled** • **Disable (Default)** The LDAP contacts feature is not available in CCMS mode.
User Name	Specifies an LDAP client user name. The default value is empty.
User Password	Specifies an LDAP client password. The default value is empty.
Server Address	Specifies the IP address or a fully qualified domain name (FQDN) of the LDAP directory server. The valid value is an IPv4 or IPv6 address in the dotted decimal format or a FQDN.
Server Port	Specifies the port number for the LDAP directory server. Valid values are positive integers from 1 to 65535. The default value is 389.
Search Base	Specifies LDAP search base parameters. Valid value is a string of parameter settings, separated by commas. For example, `dc=global,dc=avaya,dc=com`. The default value is empty.

Table continues…

Name	Description
Protocol	Specifies whether to use TLS or TCP protocol for LDAP. The options are: • **Use LDAP** • **Use LDAP+STARTTLS** • **Use LDAPS (Default)**
Authentication	Specifies the kind of authentication that is used if the value of the DIRUSERNAME parameter is not null. Value operation: • 0: Simple LDAP authentication. • 1: Simple LDAP Authentication and Security Layer (SASL).
Search Attributes	Specifies which LDAP attributes to use in contact search. Valid value is a string of LDAP server search attributes, separated by commas. The default value is `cn,sn,telephoneNumber`
Display Attributes	Specifies the LDAP attributes the phone returns in a search and the way the phone displays search attributes. Valid value is a string of LDAP search attribute names with corresponding field names, separated with commas. For example, `sn=Last Name,job title=Job,cn=Common Name,o=Office,c=Country`. The default value is empty.
Name Attributes	Specifies a primary subset of **Search Attributes** the phone displays for each match in a search list. Valid value is a string of LDAP server search attributes, separated by commas. The default value is `cn`.
Number Attributes	Specifies LDAP fields that contain a callable number. The first number in the sequence becomes the primary number. The valid value is a string of LDAP search attributes which contain a callable number, separated by commas. For example, `telephoneNumber,mobile,DoD SIP URI`. The attributes may vary from one LDAP server to another.
Custom directory label	Specifies a custom label to be used for the LDAP directory in the Contacts application. Default label is "LDAP Directory" if this value is not specified. The valid value is a string. Default value is null.

Table continues…

Name	Description
LDAP to local contact field mapping	Specifies a mapping of LDAP fields to local contact fields. The entire contact mapping is considered invalid if there is no valid rule for either first name or last name or there is no a valid rule for at least one contact number. The valid value is a string. The default value is fn=firstName,ln=lastName,cn=nickname,telephoneNumber=work
Alerting on calls	
Parked call indication	Specifies the way the phone alerts the user of BLF calls. The options are: • **0** — None • **1** — Audible • **2** — Visual • **3** — Both • **4** — Force None • **5** — Force Audible • **6** — Force Visual • **7** — Force Both
Beacon Indication mode	Specifies the way the beacon LED starts flashing when there is an incoming call. The options are: • **0** — Immediate (Default) • **1** — Delayed
Emergency Call	
Emergency Numbers	Specifies the emergency contact number. Emergency calls are not supported in an Open SIP environment.
Emergency Softkey	Specifies whether the **Emergency** soft key is displayed after the phone is registered. The options are: • **Do Not Display** • **Display without Confirmation** • **Display with Confirmation (default)**

Table continues…

Name	Description
Softkey Emergency Number	Specifies the number(s) which is dialed when the **Emergency** soft key is pressed. The valid value is up to 30 dialable characters. The default value is empty. Value format: digits from 0 to 9, *, #.
Emergency Softkey when logged out	Available only in Aura environment.
Phone Lock	
Enable Phone Lock	Specifies whether the Lock feature is enabled on the phone. The options are: • **Do Not Allow (default)** • **Allow** **Note:** If you enable the parameter, the **Lock** application is available in the **Main menu**. User can use Phone key customization to present the **Lock** application in the main phone screen. There is no **Lock** soft key or feature button. If you disable the parameter, there is no **Lock** application. User does not have the option to present the **Lock** application using Phone key customization in the main phone screen.
Phone Lock Idle Time	Specifies the idle time in minutes after which the phone is locked. The valid value is an integer from 0 to 10080. The default value is 0 minutes.
Count of PIN/password attempts	Specifies the number of failed attempts that you can permit to unlock the phone. After the user exceeds the permitted limit, the user is blocked from attempting again for a specified time. The numeric value ranges between 0–20. If you set the value to 0, the user will not be blocked for the failed attempts to unlock the phone.
Phone PIN/password lock time	Specifies the time period when the user will be blocked from attempting to unlock the phone. The numeric value ranges between 5–1440 minutes. The default value is 5 minutes.
Phone Lock PIN	Specifies the PIN that you can set to unlock the phone. The PIN must be only digits with the value ranging from 4–20 characters. The default value is null.

Table continues…

Name	Description
Audio	
Default audio path	Specifies the default audio path. Only if you set the value to either speaker or headset, the user can change the default audio path. The options are: • **Speaker (Default)** • **Headset** • **Speaker Forced** • **Headset Forced**
Call Progress Tone Country	
AGC Handset	Specifies the Automatic Gain Control setting for the handset. The options are: • **Disable** • **Enable (default)**
AGC Headset	Specifies the Automatic Gain Control setting for the headset interface. The options are: • **Disable** • **Enable (default)**
AGC Speaker	Specifies the Automatic Gain Control setting for the speaker. The options are: • **Disable** • **Enable (default)**

Table continues…

Name	Description
Handset Sidetone Level	Specifies the level of side tone in the handset. The options are: • **Normal level (default)** • **Three levels softer than Normal** • **Off** • **One level softer than Normal** • **Two levels softer than Normal** • **Four levels softer than Normal** • **Five levels softer than Normal** • **Six levels softer than Normal** • **One level louder than Normal** • **Two levels louder than Normal**
Ringtone Style	Specifies the style of the classic ring tone. The options are: • **North America (default)** • **European**
Handset Profiles	Specifies an ordered list of names to be displayed for handset audio profile selection. The list contains audio profiles set in the web interface, the `46xxsettings.txt` file and internally, for example: `Default,Normal,Amplified,Hearing Aid`. The default value is empty.
Handset Profile Default	Specifies the number of the default handset audio profile. The options are from 1 to 20. The default value is 1.
Default Acoustic Exposure Protection Mode	Specifies the acoustic exposure protection mode. The options are: • **Off (Default)** • **Dynamic** • **4 hours** • **8 hours**
Dialing	

Table continues…

Name	Description
Dial Plan	Specifies the dial plan used in the phone. Value format: a string of 0 to 1023 characters without any intervening spaces. The default value is empty.
Enable Digit Mapping	Specifies if DIGIT_MAPPING config parameter will be used for dial plan configuration, if the parameter is disabled DIALPLAN and ELD config parameters will be used. The valid values are: • **Disable (Default)**: DIALPLAN and ELD rules are applied to the dial number. • **Enable**: DIGIT_MAPPING rules are applied to the dial number.
Digit Mapping	Specifies a digit map which can be used to match digits to ensure a complete number is dialed, transform dialed digits, and block numbers from being dialed. The valid value is a string. Default value is null.
No Digit Dial Timer	Specifies the time in seconds during which the phone waits for a digit to be dialed after going off-hook and before generating a warning tone. The valid value is an integer from 0 to 60. The default value is 20 seconds.
Inter-digit Wait Timer	Specifies the time in seconds during which phone waits after a digit is dialed before sending a `SIP INVITE`. The valid value is an integer from 0 to 10. The default value is 5 seconds.
Dial Local Area Code	Specifies whether the user must dial the area code of calls within the same area code regions. The options are: • **No (default)** • **Yes**
Local Area Code	Indicates the phone local area code which allows the user to dial local numbers with more flexibility. The valid value is a sting of 5 digits ranged from 0 to 9. The default value is empty.

Table continues…

Name	Description
Default dialing mode	Specifies the dialing mode for the user. If this parameter is set to Automatic or Manual, then it specifies default dialing mode. If this parameter is set to forced, then the option to pick dialing mode is not available on the phone UI for the user. The valid values are: • **Automatic** • **Manual (Default)** • **Automatic Forced** • **Manual Forced**
Ringtones	
Primary Ringtone	Displays a list of ringtones for you to select a default ringtone for the primary incoming calls. These incoming calls are not associated with any other ringtone based on the call type or a contact association.
Call Forward Ring	Displays a list of ringtones for you to select a default ringtone for notification of a forwarded incoming call from another phone.
Ring Reminder	Displays a list of ringtones for you to select a default ringtone for the ring reminder incoming calls. Available only in the Open SIP servers that support this feature.
Call Park	Displays a list of ringtones for you to select a default ringtone for notification of a parked call on the logged-in extension.
BLF Incoming Call	Displays a list of ringtones for you to select a default ringtone for notification of an incoming call on a BLF. Available only in the Open SIP servers which support this feature.
BLF Call Park	Displays a list of ringtones for you to select a default ringtone for notification of a parked call on a BLF. Available only in the Open SIP servers which support this feature.
Priority Alert	Displays a list of ringtones for you to select a default ringtone for notification of an incoming priority call.
Alternate Number 1	Displays a list of ringtones for you to select a default ringtone for notification of an incoming call from the first alternate number. Available only in a BroadSoft environment.
Alternate Number 2	Displays a list of ringtones for you to select a default ringtone for notification of an incoming call from the second alternate number. Available only in a BroadSoft environment.

Table continues…

Name	Description
Alert-Info Ringtones	Allows you to assign specific ringtones to incoming calls on specific ACD queues. Available in the following environments: • Netsapiens • Metaswitch • FreeSWITCH • Asterisk
Show or Hide Ringtones on the Phone User Menu	
Primary Ringtone Menu Item	Specifies whether the primary ringtone menu item is displayed in the phone user menu. The options are: • **Show (Default)** • **Hide**
Ring Reminder Ringtone Menu Item	Specifies whether the ring reminder ringtone menu item is displayed in the phone user menu. The options are: • **Show (Default)** • **Hide**
Call Park Ringtone Menu Item	Specifies whether the call park ringtone menu item is displayed in the phone user menu. The options are: • **Show (Default)** • **Hide**
BLF Incoming Call Ringtone Menu Item	Specifies whether the BLF incoming call reminder ringtone menu item is displayed in the phone user menu. The options are: • **Show (Default)** • **Hide**
BLF Call Park Ringtone Menu Item	Specifies whether the BLF call ringtone menu item is displayed in the phone user menu. The options are: • **Show (Default)** • **Hide**

Table continues…

Name	Description
Priority Alert Ringtone Menu Item	Specifies whether the priority alert ringtone menu item is displayed in the phone user menu. The options are: • **Show (Default)** • **Hide**
Alternate Number 1 Ringtone Menu Item	Specifies whether the alternate number 1 ringtone menu item is displayed in the phone user menu. The options are: • **Show (Default)** • **Hide**
Alternate Number 2 Ringtone Menu Item	Specifies whether the alternate number 2 ringtone menu item is displayed in the phone user menu. The options are: • **Show (Default)** • **Hide**
Enhanced Local Dialing Rules	
Enable Local Dialing Rules	Specifies whether the algorithm defined by parameters in this section is used during certain dialing procedures. The options are: • **Disable** • **Enable without Contacts (default)** • **Enable with Contacts**
Country Code	Specifies the country code of the phone. The valid value is an integer from 1 to 999. The default value is 1.
International Access Code	Specifies the international access code. The valid value is up to 4 dialable characters. The default value is 011. Value format: digits from 0 to 9, *, #.
Long Distance Access Code	Specifies the long distance access code. The valid value range is a sting of integers from 0 to 9, and empty. The default value is 1.
Dial Access Code	Specifies the dial access code that is applied if the dialed number length + Dial access code length equals the national number length. This calculation does not include an outside line access code. The default value is null.

Table continues…

Name	Description
Internal Extension Number Length	Specifies the length of an internal extension number. The valid value is an integer from 3 to 13. The default value is 5.
National Telephone Number Length	Specifies the length of a national phone number. The valid value is an integer from 5 to 15. The default value is 10.
Outside Line Access Code	Specifies the number for making an outside call, i.e. a local call in a public network. The valid value is up to 2 dialable characters. The default value is 9. Value format: digits from 0 to 9, *, #.
Remove PSTN access prefix from outgoing number	Allows dialing digits during failover and removing of the PSTN access prefix from the outgoing number. The options are: • **No (default)** • **Yes**
Admin	
Admin Access allowed from Phone	Specifies whether the administrative procedures are used for the phone configuration. The options are: • **Yes (default)** • **No**
Admin Login fail attempt allowed	Specifies the number of failed attempts to enter the Administration access code before the login is locked. The options are from 1 to 20. The default value is 10.
Lockout time after failed Admin Login attempt	Specifies the time interval in minutes to re-enter the Administration access code after the login is locked. The valid value is an integer from 5 to 1440. The default value is 10 minutes.
MLPP	
Enable MLPP	Specifies whether the MLPP feature is enabled. The options are: • **Disable (default)** • **Enable**
Maximum Precedence Level	Specifies the maximal allowed precedence level for the user. The options are from 1 to 5. The default value is 1.

Table continues…

Name	Description
MLPP Network Domain	Specifies the MLPP Network domain. The valid values are: empty, “uc” and “dsn”. The default value is empty.
MLPP Precedence Domain	Specifies the MLPP Precedence domain. The valid values range between 0-9, A-F. The default value is 000000.
Enable Precedence Softkey	Controls whether the **Precedence** soft key should be displayed on idle line appearances on the phone screen. The options are: • **Disable** • **Enable (default)**
Guest Login	
Guest Login Enable	Specifies whether the Guest Login feature is available on the phone. The options are: • **Disable (default)** • **Enable**
Guest Login Session Duration (hours)	Specifies the time interval in hours before a guest or a visiting user will be automatically logged off if the telephone is idle. The valid value is an integer from 1 to 12. The default value is 2 hours.
Guest Login Session Warning Time (minutes)	Specifies the time interval in minutes before a warning of the automatic logoff is initially displayed for a guest or a visiting user. The valid value is an integer from 1 to 15. The default value is 5 minutes.
Save Extension	
Show Last Extension	Specifies whether the extension is displayed after logging out. The options are: • **Disable (default)** • **Enable**
Bluetooth	
Bluetooth Enable	Specifies whether Bluetooth can be enabled in the phone menu. The options are: • **Disable** • **Enable (default)**

Table continues…

Name	Description
CCMS	
Media Preservation	Specifies whether a call will be preserved when there is no SIP connectivity to IP Office. This setting is applied only in the Avaya Aura® environment. The options are: • **Disable** • **Enable (default)**
Preserved Call Duration	Specifies the time interval in minutes during which the call is preserved. To apply this setting, **Enable IP Office** should be set to **CCMS** and **Media Preservation** should be enabled. This setting is applied only in the Avaya Aura® environment. The valid value is an integer from 10 to 120. The default value is 120 minutes.
Brightness	
Primary Display Brightness	Adjusts the brightness of the phone primary display. The options are from 1 to 5. The default value is 4.
Secondary Display Brightness	Adjusts the brightness of the phone secondary display. The options are from 1 to 5. The default value is 4.
Button Module #1 Display Brightness	Adjusts the display brightness of the first attached button module. If no button modules are attached to the phone, this field is disabled. The options are from 1 to 5. The default value is 4.
Button Module #2 Display Brightness	Adjusts the display brightness of the second attached button module. If no button modules are attached to the phone, this field is disabled. The options are from 1 to 5. The default value is 4.
Button Module #3 Display Brightness	Adjusts the display brightness of the third attached button module. If no button modules are attached to the phone, this field is disabled. The options are from 1 to 5. The default value is 4.
USB This option is available only in Avaya J159 IP Phone and Avaya J189 IP Phone	

Table continues…

Name	Description
USB Power	Controls USB power when power is provided to the USB interface. The valid values are: • **0-OFF**: turn off USB power. • **1-ON**: turn On USB power only if Aux powered. • **2-ON (Default)**: turn On USB power. • **3-ON**: turn On USB power if Aux powered or PoE slide switch is set high.
USB Headset	Specifies whether to enable or disable USB Headset. The valid values are: • **Enabled (Default)** • **Disabled**
USB Keyboard	Specifies whether to enable or disable USB keyboard. It allows to use the keyboard to enter texts. The valid values are: • **Enabled (Default)** • **Disabled**
USB Stick	Specifies whether to enable or disable USB stick. It allows to copy phone reports to flash drive. The valid values are: • **Enabled (Default)** • **Disabled**
Privacy	
GDPR Mode	Specifies whether the Secure mode is applied on the phone. The options are: • **Enable (default)** • **Disable**
Downloadable Directory	
Downloadable Directory File Name	Enter the directory file name. The .xml file is the file which has the global directory contacts details and is stored in the file server.
Presence	

Table continues…

Name	Description
System DND Link	Specifies one of the following: • Activate the SendAllCall feature when the user enables DoNotDisturb presence. • Activate DoNotDisturb presence when the user enables the SendAllCall feature. • Activate a one-way link between the SendAllCall feature and DoNotDisturb presence. • Disable all links. The options are: • **No link (Do not activate SendAllCall when user enables DoNotDisturb) (Default)** • **One way link (Activate SendAllCall when user enables DoNotDisturb)** • **Two way link (Activate SendAllCall when user enables DoNotDisturb and vice versa)** • **Forced- No link (Do not activate SendAllCall when user enables DoNotDisturb) (Default)** • **Forced- One way link (Activate SendAllCall when user enables DoNotDisturb)** • **Forced- Two way link (Activate SendAllCall when user enables DoNotDisturb and vice versa)**
Avaya Spaces	
Spaces Access Mode	Specifies the authentication mode that can be used by the phone when connecting to Avaya Spaces. The options are: • **Disabled**: all Avaya Spaces features via APIs are disabled. • **Guest only (Default)**: Avaya Spaces feature can be accessed by guest/anonymous authentication only. Connections to Avaya Spaces uses the embedded public certificates and any certificates defined in the TRUSTCERTS. It ignores ENABLE_PUBLIC_CA_CERTS.

Table continues…

Name	Description
Spaces URL	Specifies URL to Avaya Spaces service. The value starts with http:// or https://. The default scheme is https://. The value length is 0- 255 characters without space. The default value is https://spaces.avayacloud.com/ **Warning:** Do not change this parameter unless instructed by Avaya Support.
Spaces API URL	Specifies URL to Avaya Spaces API service. The value starts with http:// or https://. The default scheme is https://. The value length is 0- 255 characters without space. The default value is https://spacesapis.avayacloud.com/api/ **Warning:** Do not change this parameter unless instructed by Avaya Support.
Spaces Direct Number	You can define a direct number to use when attempting a call to Avaya Spaces. If the user does not select an Avaya Spaces direct number then this defined direct number is used. The value length is up to 32 characters. Can contain the following: 0 to 9 digits, minus (-), parenthesis ((), plus (+). The default value is Empty.
Spaces Direct Number Menu Item	Specifies if the end user is allowed to select a direct number for a voice call to Avaya Spaces. The options are: • **Hide**: user is not allowed to select a direct number for a voice call to Avaya Spaces. Any previously selected direct number by the end user is cleared. If **Spaces Direct Number** is not defined or found to not exist as a valid Direct Number, the user sees an error and warning pop-up on the phone screen. • **Show (Default)**: user is allowed to select a direct number for a voice call to Avaya Spaces. WLAN_COUNTRY is used to determine the location of the phone. The phone displays phone numbers based on this location. If you set the parameter WLAN_COUNTRY to a country that does not exist in the list of numbers provided by Avaya Spaces, then the phone number of the US is shown.
Other	

Table continues…

Name	Description
Softkey Configuration	Specifies which feature will show up on which soft key on the phone screen. This setting applies only to Avaya J129 IP Phone. The following numbers are assigned to the features: • 0 – Redial • 1 – Contacts • 2 – Emergency • 3 – Recents • 4 – Voicemail Value format: numbers from 0 to 4 and a comma (,). The default value is “0,1,2”.
Branding Volume	Specifies the volume level at which the Avaya audio brand is played. The options are: • **12db below nominal** • **9db below nominal** • **6db below nominal** • **3db below nominal** • **Nominal (default)** • **3db above nominal** • **6db above nominal** • **9db above nominal**
Phone Mute Alert	Specifies whether the Mute Alert feature is blocked. The options are: • **Unblocked** • **Blocked (default)**
Extend Ringtone	Specifies the audio files to customize the ring tone. Value format: the list of file names in `.xml` format separated by commas. The default value is empty.
Group Number	Specifies group numbers if available. The valid value is an integer from 0 to 999. The default value is 0.

Table continues…

Name	Description
Minimum delay to backup volume level to PPM	Specifies the minimal time in seconds between backups of the volume levels to the PPM service when the phone is registered to Avaya Aura® Session Manager. The valid value is an integer from 0 to 900. The default value is 2.
Ignore Contact Header Display Name	Specifies blocking of display name from Contact header. The options are: • **Do not ignore (Default)** • **Ignore**
Forwarded by order	The "Forwarded by" details are shown for incoming calls that have been forwarded by another user. Specifies which user information to be displayed on an incoming call if there are multiple forwards before being received as an incoming call. The options are: • **First Forwarded (Default)**: First user to have forwarded is shown as the Forwarded By User. • **Last Forwarded**: Last user to have forwarded is shown as the Forwarded By User.
Home Idle Timeout	Specifies that the phone activates the home view if it remains idle for the specified period of time (in minutes) The options are: • Minimum value is 0 , the feature is disabled • Maximum value is 30 • Default value is 10 minutes
Application Header Appearance Context	Specifies whether appearance context should be displayed on application header line on Phone Screen. The options are: • **Disable** • **Enable** The default value is null.

Configuring date and time

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Date & Time**.

3. In the Daylight Saving section, configure the following:
   - **Daylight Saving Mode**: Select one of the following options:
     - **No daylight saving time**
     - **Manual daylight savings activated (time set to DSTOFFSET)**
     - **Automatic daylight savings adjustment (as specified by DSTSTART and DSTSTOP) (Default)**
   - **DST Offset**: Specifies the time in hours between the standard time and daylight savings time. Select one of the following options:
     - **0**
     - **1 hour (default)**
     - **2 hours**
   - **DST Start**: Specifies when to apply the offset for daylight savings time. The value format must be either `odddmmmht` or `Dmmmht`, where:
     - `o` represents a one-character ordinal adjective. For example, 1 for first, 2 for second, 3 for third, 4 for fourth, or L for last.
     - `D` represents 1 or 2 ASCII digits or characters representing the date of the month.
     - `ddd` represents three characters containing the English abbreviation for the day of the week. For example, Sun for Sunday, Mon for Monday, etc.
     - `mmm` represents a three-character English abbreviation for the month. For example, Jan for January, Feb for February, etc.
     - `h` represents a one-numeric digit representing the time to make the adjustment at hAM (0h00 in military format).

       The valid values of `h` are from 0 to 9.
     - `t` represents one character for the time zone to which the changes are applied. For example, “L” for local time or “U” for Universal Time.
   - **DST Stop**: Specifies when to stop the offset for daylight saving time. The value format must be either `odddmmmht` or `Dmmmht`, where:
     - `o` represents a one-character ordinal adjective. For example, 1 for first, 2 for second, 3 for third, 4 for fourth, or L for last.
     - `D` represents 1 or 2 ASCII digits or characters representing the date of the month.
     - `ddd` represents three characters containing the English abbreviation for the day of the week. For example, Sun for Sunday, Mon for Monday, etc.
     - `mmm` represents a three-character English abbreviation for the month. For example, Jan for January, Feb for February, etc.
     - `h` represents a one-numeric digit representing the time to make the adjustment at hAM (0h00 in military format).

The valid values of `h` are from 0 to 9.

- `t` represents one character for the time zone to which the changes are applied. For example, “L” for local time or “U” for Universal Time.

4. Click one of the following:
   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.

Next steps

Note:

The phone can obtain date and time from an NTP server. If an NTP server is not configured or cannot be accessed, a SIP server is used. If the phone operates in CCMS mode in IP Office environment and connects to the SIP server to get date and time and displays incorrect date and time values, the SIP server may have an incorrect or inaccurate date and time configuration.

Configuring management settings

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Management**.
3. Configure the parameters in the following sections:
   - Device Enrollment Service
   - Plug and Play (PNP) Provisioning
   - Configuration
   - Firmware
   - Backup/Restore User Data
   - Updates
4. Click one of the following:
   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.

Management settings field descriptions

Name	Description
Device Enrollment Service	

Table continues…

Name	Description
DES Discovery	Specifies the DES Discovery mode. The options are: • **Enable (default)** • **Disable** • **Disable and Restored with Reset to Default** • **Force enable on DES prompt timeout**
Embedded Public Certificates	Specifies whether to trust the embedded public certificates. The options are: • **Trusted only if Trustcerts is empty (default)** • **Always Trusted**
Plug-and-Play (PNP) Provisioning	
PNP Configuration	Specifies the status of the PNP configuration. The options are: • **Enabled (default)** • **Disabled**
Configuration	
PPM Server Access Mode	Specifies the server access mode of the provisioning server. The options are: • **HTTP** • **HTTPS (default)** **Note:** Use HTTPS if the SIP transport mode is TLS, otherwise, use HTTP.
Download Settings file using HTTPS only	Specifies whether only HTTPS is used to download the settings file. The options are: • **Yes** • **No (default)**

Table continues…

Name	Description
Import Settings File	Enables the user to import the settings file. To import the settings file, click **Browse** to browse your local PC or any PC connected to the network. Select the file and click **Import**. Restart the phone for new parameters from the settings file to take effect.
Export Settings File	Enables the user to export a configuration file. To export the configuration file, click **Export**.
Firmware	
Software Version	Displays the version of the SIP software. This field is empty by default.
Backup Software Version	Displays the backup software version. This field is empty by default.
Firmware Upgrade	You can import the firmware upgrade file from a local PC or any PC connected to the network. To upload the firmware upgrade file, click **Browse** to browse your PC, select the file and click **Upgrade**. After you click **OK** in the prompt, the phone downloads the new firmware and then reboots.
Backup/Restore User Data	
User store Address for Backup/Restore	Specifies the HTTP and HTTPS IP address or the DNS name of the storage location to backup and retrieve data. The valid value starts with `http://` or `https://` and contains either an IP address or a DNS name without any intervening spaces. The maximal value length is 255 characters.
Updates	
Automatic Update Policy	Specifies daily, or days of week, or days month to apply automatic update policy on the phone to download settings & firmware changes automatically. The options are: • **Disabled (Default)** • **Daily** • **Weekly** • **Monthly**

Table continues…

Name	Description
Automatic Update Days	Specifies the day or days of the week on which the settings & firmware should update automatically. The default value is null.
Automatic Update Window	Specifies hours of a day in 24h format during which phone should download settings & firmware changes automatically. The default value is 2,4.
Automatic Update Reboot Prompt	Specifies to prompt the user if device reboot is required for new settings or firmware update. The options are: • **Don't prompt user (Default)** • **Prompt user if reboot due to new settings or firmware is required**
Automatic Firmware Upgrade Only After	Specifies the date and time after which new firmware is downloaded and installed. After this date and time is reached, the phone uses the settings of **Automatic Update Days** and **Automatic Update Window** to trigger the reboot for firmware download. If this parameter value is not set, then phone uses **Automatic Update Policy**, **Automatic Update Days**, and **Automatic Update Window** to trigger the firmware download. The format is YYYY-MM-DDThh:mm, where YYYY is 4 digit numeric value for year, MM is 2 digit numeric value for Month, DD is 2 digit numeric value for date, which is 1 to 31. T is the time separator, hh is 2 digit numeric value for hours of the day, which is 00 to 23. mm is 2 digit numeric value for minutes of the hour, which is 00 to 59. The default value is null. An example value is 2020-12-13T12:12
Manual Update Settings	Specifies to apply new settings or upgrade the phone to a new firmware version. Click **Update**, and then click **OK**. The phone checks for updates and depending on the files stored in file server directory, restarts or upgrades to a new firmware version.

Changing the password of the phone Administrator menu

About this task

You can change the administrator password for the Administration menu on the phone.

The administration password must be between 6 to 31 alphanumeric characters. You can use special characters such as: tilde (~), exclamation mark (!), at (@), pound (#), dollar ($), percent (%), carat (^), ampersand (&), asterisk (*), underscore(_), minus (-), plus (+), equal (=), back quote (`), pipe (|), parenthesis (()), braces ({}), brackets ([]), colon (:), semicolon (;).

Procedure

1. Log in to the web interface by using your username and current password.
2. In the navigation pane, click **Password**.
3. In the **Phone Administration Menu Password** section, do the following:
   a. Enter the web administrator password in the **Web Administrator Password** field.
   b. Enter the new password in the **New Password** field.
   c. Re-enter the new password in the **Confirm Password** field.
   d. Click **Save**.

Debugging

About this task

You can debug the phone using the fields listed under the Debugging tab of the phone web interface.

Before you begin

Enable access to the web interface of the phone.

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Debugging**.
3. Configure the fields in the following areas:
   - Log
   - SNMP
   - Packet Capture
   - Phone Report
   - SSH
   - Long Term Acoustic Protection
   - Other
4. Click one of the following:
   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.

Related links

Enabling Debugging on the Avaya J179 IP Phone

Debugging field descriptions

Name	Description
Log	
Logging	Specifies the logging status. The options are: • **Off (default)** • **On**
Syslog Server	Specifies the IP or the DNS address of the Syslog server. For secure syslog mode, you must use an FQDN address. The valid value is a string of up to 255 ASCII characters. The default value is empty.
Log Server Secure	Specifies if a secure or non-secure mode is selected as default for syslog messages transportation. The options are: • **Off (default)** • **On**
Syslog Level	Specifies the severity level of the syslog messages. Events with the selected severity level and above are logged. The options are: • **Emergencies (default)** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notices** • **Information** • **Debug**
Log Categories	Specifies the list of log categories. Select the appropriate log category. For example, select category **Audio** for generating audio logs. The default value is empty.

Table continues…

Name	Description
Enhanced Debugging	Specifies the status of enhanced debugging. The options are: • **Enable** • **Disable (default)**
SNMP	
SNMP String	Specifies the SNMP community name string. The valid value is a string of up to 32 ASCII alphanumeric characters. The default value is empty.
SNMP Address	Specifies the IP addresses for SNMP queries. The valid value is a string of up to 255 ASCII characters without any intervening spaces. The default value is empty.
Packet Capture	
Packet Capture	Captures the phone network traffic. See Capturing the phone network traffic on page 195
Phone Report	
Phone Report Server Address	Specifies the file server address to send the phone report. Click **Generate Phone Report**. The valid value is a string of up to 255 ASCII characters. **Note:** The phone report also provides details such as product ID, default server type, and DES support information.
SSH	
SSH Allowed	Specifies whether Secure Shell (SSH) is supported. The options are: • **Enable** • **Disable (default)** • **Configured using local administrative procedure**
SSH Idle Timeout	Specifies the time in minutes after which SSH is disabled. The valid value is an integer from 1 to 32767. The default value is 10 minutes.
SSH Banner File	Specifies the file name or the URL for a custom SSH banner file. The valid value is a string of up to 255 ASCII characters. The default value is empty.

Table continues…

Name	Description
EASG site certificates	Specifies the list of EASG site certificates. Support technicians use these certificates to generate EASG responses for SSH login without access to the Avaya network. The valid value is a string of up to 64 ASCII characters. The default value is empty. **Note:** You can add a maximum of four certificates.
EASG site Authentication Factor code	Specifies the Site Authentication Factor code associated with the EASG site certificate installed. The valid value is a string of 10 to 20 alphanumeric characters. The default value is empty.
Days before EASG certificates expiration warning	Specifies the number of days before the expiration of the EASG product certificate that a warning message first appears on the phone screen. The valid value is an integer from 90 to 750. The default value is 365.
SLA Monitor	
SLA Monitor Agent	Specifies the status of the SLA Monitor Agent. The field displays the value as set in the `46xxsettings.txt` file.
SLA Monitor Server Address	Specifies the IP address of the SLA Monitor server. The Valid value is in the dotted-decimal name format. The default value is “0.0.0.0:0”. The field displays the value as set in the `46xxsettings.txt` file.
Packet Capture (sniffing)	Specifies whether the SLA Monitor agent supports packet capture. The field displays the value as set in the `46xxsettings.txt` file. The options are: • **Disable (default)** • **Enable with payloads removed from RTP packets** • **Enable with payloads included in RTP packets** • **Controlled from Admin Menu**
Device Control	Specifies whether the SLA Monitor agent supports device control. The field displays the value as set in the `46xxsettings.txt` file. The options are: • **Disable (default)** • **Enable** • **Controlled from Admin Menu**

Table continues…

Name	Description
Device Performance Monitoring	Specifies whether the SLA Monitor agent supports access to phone performance data. The field displays the value as set in the `46xxsettings.txt` file. The options are: • **Enable** • **Disable (default)**
UDP Port for discovery and test messages	Specifies the port used to receive packets from an SLA Monitor server. The valid value is an integer from 6000 to 65535. The default value is 50011. The field displays the value as set in the `46xxsettings.txt` file.
Long Term Acoustic Protection	
Feature Mode	Specifies the dynamic evaluation of the acoustic protection. The valid values are: • **Production (Default)**: the dynamic evaluation of the acoustic protection is active. • **Debugging**: the dynamic evaluation of the acoustic protection is inactive.
Acoustic exposure config mode	Specifies the acoustic exposure dynamic range. The valid values are: • **Acoustic protection off (Default)** • **Acoustic protection On (Default)**
Sliding Window Size	Specifies the window size for acoustic protection. The valid value ranges from 8 to 1440 Minutes. The default value is 480 minutes.
Other	
Serial Port	Specifies if the port for network traffic is enabled or disabled. The options are: • **Adjunct** • **Disable** The default value is Adjunct.

Capturing the phone network traffic

About this task

You can capture the real-time network traffic of the phone using the phone web interface. You receive the network traffic data on the computer from where you launch the phone web interface. When you start the process of capturing the network traffic, the phone sends the traffic data to the

browser, and after you end the process, the final .pcap file is created on your computer. You can also capture the network traffic when your phone is on an active Wi-Fi connection. The packet capture file has data only if there is active network traffic while you run the report.

You can use the phone network traffic data to debug the phone registration and call-related issues.

Before you begin

Ensure your phone is on an active network connection.

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Debugging**.
3. Scroll to the **Packet Capture** section.
4. Press **Start**.

   The packet capture file starts downloading in a location per your browser setting.

   The file name format is <device model><MAC address ><timestamp>.pcap
5. Press **Stop** to end the packet capture.

   While you are running the report, the packet capture also stops in the following scenarios:

   - If you log out of the phone web interface.
   - If the phone web interface session times out.
   - If you log in to the same phone web interface in another browser instance.

   We recommend using IPv4 for the Avaya J129 IP Phone for the seamless performance of this feature.

Configuring certificates

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Certificates**.
3. Configure the following areas:
   - Certificates
   - Online Certificates Status Protocol (OCSP)
   - SCEP
   - PKCS12
4. Click one of the following:
   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.

Certificates field descriptions

Name	Description
Certificates	
Upload Trusted Certificate	Specifies the trusted certificate used by the phone. You can also browse and upload the certificates from the local PC by clicking **Browse** > **Import**.
Trusted Certificates file to upload	Specifies the name of the certificate file to be uploaded. The valid value is a string up to 255 ASCII characters. File names must be separated by commas without any intervening spaces. The default value is empty.
Match Identity to trust certificate	Specifies the status of the TLS server identification. The options are: • **Yes (Default)** • **No**
RFC 5922 certificate compliance	Specifies whether to enable or disable validating the SIP server certificate for RFC 5922 compliance. The options are: • **Enable (Default)** • **Disable**
Require Key Usage certificate extension	Specifies whether to enable or disable checking for Key Usage extensions. The options are: • **Enable (Default)** • **Disable**
Server Certificate re-check hours	Specifies the time interval in hours for rechecking the expiration and revocation status of the certificates used to establish any existing TLS connections. The valid value is an integer from 0 to 32767. The Default value is 24 hours.
Warning on number of days before Certificate expiration	Specifies the number of days before the expiration of a certificate that a warning must first appear on the phone screen. The valid value is an integer from 0 to 99. The Default value is 60 days.

Table continues…

Name	Description
FQDN IP Mapping	Specifies a FQDN contained in the certificate when an IP address is used to establish the connection. The parameter is a comma-separated list of names or value pairs where the name is an FQDN and the value is an IP address. The valid value is a string of up to 255 characters without any intervening spaces. The Default value is empty.
Online Certificate Status Protocol (OCSP)	
Enable OCSP	Specifies the status of OCSP. The options are: • **Disable (Default)** • **Enable**
Action on Unknown Revocation Status	Specifies whether a certificate is authenticated when its revocation status cannot be determined. The options are: • **Certificate revocation operation will accept certificates (Default)** • **Certificate is considered to be revoked and TLS connection is closed**
Nonce in OCSP Request	Specifies whether a nonce is added to OCSP requests and expected in OCSP responses. The options are: • **Do not add** • **Add (Default)**
OCSP Address	Specifies a URI for an OCSP responder. The URI can be an IP address or a host name. The valid value is a string of up to 255 characters without any intervening spaces. The default value is empty.
OCSP Address Preferred	Specifies the preferred OCSP responder URI. The options are: • **Use OCSP address configured first and then OCSP field of AIA extension of the certificate being checked (Default)** • **Use OCSP field of AIA extension of the certificate being checked first and then OCSP address configured**

Table continues…

Name	Description
OCSP Trusted Certificates	Specifies the trusted OCSP certificates to be downloaded. It also acts as a separate trusted certificate repository for the OCSP Trusted Responder Model and contains certificates that the OCSP responder can trust. This value is required if the OCSP responder uses a different CA for the server certificate than the root CA. The valid value is a string of up to 255 characters without any intervening spaces. The default value is empty.
OCSP Hash Algorithm	Specifies the hashing algorithm for an OCSP request. value operation. The options are: • **SHA-1 (Default)** • **SHA-256**
Use OCSP Caching	Specifies whether OCSP caching is in use. The options are: • **Yes (Default)** • **No**
OCSP Cache Expiry	Specifies the time interval in minutes for the OCSP cache expiry. The valid value is an integer from 60 to 10080. The default value is 2880 minutes.
SCEP	
SCEP Server	Specifies the URL address of the SCEP server. The valid value is a string of up to 255 ASCII characters without any intervening spaces. The default value is empty.
Common Name	Specifies the common name for the subject in an SCEP certificate request. The valid value is a string of up to 255 ASCII characters without any intervening spaces. The default value is “$SERIALNO”.
Subject	Specifies the part of SUBJECT in an SCEP certificate request that is common for requests from different device. For example, Organizational Unit, Organization, Location, State, and Country. The valid value is a string of up to 255 ASCII characters without any intervening spaces. The default value is empty.

Table continues…

Name	Description
CA Identifier	Specifies the Certificate Authority Identifier. Certificate Authority servers may require a specific CA Identifier string to accept GetCA requests. If the device works with such a Certificate Authority, the CA identifier string can be set through this parameter. The valid value is a string of up to 255 ASCII characters without any intervening spaces. The default value is “CAIdentifier”.
Initiate renewal on % of Validity Interval	Specifies the percentage of the identity certificate’s Validity interval after which renewal procedures will be initiated. If the renewal time interval has elapsed, the phone starts to contact the SCEP server periodically to renew the certificate. The valid value is an integer from 1 to 90. The default value is 90 percent.
Phone behavior on Pending request	Specifies the functioning of the device when performing certificate enrolment. The options are: • **Poll SCEP server periodically in background** • **Wait until a certificate is received or rejected (Default)**
SCEP Password	Specifies a challenge password to use with SCEP. The valid value is a string of up to 255 ASCII characters without any intervening spaces. The default value is “$SERIALNO”.
PKCS12	
PKCS12 Address	Specifies the IPv4 or IPv6 URL address, or FQDN from where a PKCS#12 file is to be downloaded. The valid value is a string of up to 255 ASCII characters without any intervening spaces. The default value is empty.
PKCS12 Password Retry Count	Specifies the number of attempts allowed for password entry. The valid value is an integer from 0 to 100. The default value is 3 attempts.
Available Identity Certificate	Specifies the trust certificates used as trust points for TLS connections.
Upload Identity Certificate	Displays available trust certificates for the phone. You can also browse and upload the certificates from the local PC by clicking **Browse** > **Import**.

Configuring Environment Settings

Procedure

1. Log in to the web interface.

2. In the navigation pane, click **Environment Settings**.
3. In the Environment Setting area, enable the required environment:
   - **AURA environment**: To set Avaya Aura as your environment.
   - **Discover AVAYA environment**: To discover whether the phone supports Avaya Aura SIP AST feature.
   - **IP Office Environment**: To set IP Office as your environment.
   - **3PCC Environment**: To set Open SIP as your environment.
   - **3PCC Server Mode**: To set an operation mode in an Open SIP environment.
4. Click one of the following:
   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.

Configuring Background and Screen Saver of the Phone

About this task

You can configure the background and screen saver of the phone using the web interface for all the models of Avaya J100 Series IP Phones except Avaya J129 IP Phone.

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Background and Screen Saver**.
3. Configure the fields of the following sections:
   a. Background Image
   b. Screen Saver
4. Click one of the following:
   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.

Background Image and Screen Saver field description

Name	Description
Background Image	

Table continues…

Name	Description
Primary Background Image Selectable by User	Specifies whether the user can select a primary background image. The options are: • **Enable (default)** • **Disable**
Selected Primary Background Image	Specifies the file name of the selected primary background image. The file name must be from the list of background images (see **Primary Background Image List** below). The valid value is a string of up to 255 characters. The default value is empty.
Primary Background Image List	Specifies the list of primary background images. The valid value is a string of up to 255 characters separated by commas without any intervening spaces. The default value is empty.
Secondary Background Image Selectable by User	Specifies whether the user can select a secondary background image. The options are: • **Enable (default)** • **Disable**
Selected Secondary Background Image	Specifies the file name of the selected secondary background image. The file name must be from the list of background images (see **Secondary Background Image List** below). The valid value is a string of up to 255 characters. The default value is empty.
Secondary Background Image List	Specifies the list of secondary background images. The valid value is a string of up to 255 characters separated by commas without any intervening spaces. The default value is empty.
Screen Saver	
Primary Screen Saver Image Selectable by User	Specifies whether the user can select the primary screen saver image. The options are: • **Enable (default)** • **Disable**

Table continues…

Name	Description
Selected Primary Screen Saver Image	Specifies the file name of the selected primary screen saver image. The file name must be from the list of screen saver images (see **Primary Screen Saver Image List** below). The valid value is a string of up to 255 characters. The default value is empty.
Primary Screen Saver Image List	Specifies the list of primary screen saver images. The valid value is a string of up to 255 characters separated by commas without any intervening spaces. The default value is empty.
Secondary Screen Saver Image Selectable by User	Specifies whether the user can select the secondary screen saver image. The options are: • **Enable (default)** • **Disable**
Selected Secondary Screen Saver Image	Specifies the file name of the selected secondary screen saver image. The file name must be from the list of screen saver images (see **Secondary Screen Saver Image List** below). The valid value is a string of up to 255 characters. The default value is empty.
Secondary Screen Saver Image List	Specifies the list of secondary screen saver images. The valid value is a string of up to 255 characters separated by commas without any intervening spaces. The default value is empty.

Configuring Calendar of the phone

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Calendar**.
3. Configure Exchange Calendar.
4. Click one of the following:
   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.

Exchange Calendar field description

Name	Description
Exchange Calendar	
Provide Calendar	Specifies whether the Exchange Calendar menu is available on the phone. The options are: • **Enable (Default)** • **Disable**
Admin Configured Authentication Method	Specifies the Exchange authentication method configured by administrator. When you configure Basic (Forced) or OAuth (Forced) method, it is the active authentication method. The phone user is not allowed to change the authentication method from phone user interface. When you configure non-forced method, phone user can change the authentication method from the phone user interface and configure the active authentication method. The options are: • **Basic (Default)** • **OAuth** **Basic (Forced)** **OAuth (Forced)**
User Account Default (OAuth only)	Specifies the Exchange user account configured by administrator. This parameter is only applicable when authentication method is OAuth. If phone user hasn't configured any user name on the phone user interface then value configured in this parameter would be used. The valid value is a string of up to 255 characters. The default value is empty.
User Domain (Basic only)	Specifies the user domain for Microsoft Exchange Server. The valid value is a string of up to 255 characters. The default value is empty.

Table continues…

Name	Description
Email Domain	Specifies the Exchange email domain for Microsoft Exchange Server. The valid value is a string of up to 255 characters. The default value is empty.
Server List	Specifies a list of one or more Exchange server IP addresses. The valid value must be in the dotted decimal name format or DNS name format without any intervening spaces. The maximal value length is 255 characters. The default value is empty.
Server Secure Mode	Specifies the exchange server mode. The options are: • **HTTP** • **HTTPS (default)**

Configuring Multicast Paging

About this task

Use this procedure to enable or disable Multicast Paging on the phone and configure the settings for transmission.

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Multicast Paging**.
3. In the Multicast Paging tab, configure the following fields:
   - **Multicast Paging State**
   - **Multicast Paging Codec**
4. Configure the incoming and outgoing paging groups in the following sections:
   - Multicast Paging Groups To Listen
   - Multicast Paging Groups To Send
5. Click one of the following:
   - **Save**: To save the changes.
   - **Reset to Default**: To revert to the default values.

Related links

Multicast Paging on page 315
Multicast Paging configuration on page 316

Multicast Paging field description

Name	Description
Multicast Paging State	Specifies whether the Multicast Paging feature is enabled on the phone. If Multicast Paging state is not set, other settings related to the feature will be ignored. The options are: • **Enable** • **Disable (default)**
Multicast Paging Codec	Specifies a codec which will be used in Multicast Paging transmissions. The options are: • **G.729 (default)** • **G.711u** • **G.711a**
Multicast Paging Groups To Listen	If the Multicast Paging feature is enabled, you can add, edit or delete incoming multicast page groups in this section. The configuration fields are equivalent to the MP_GROUPS_TO_LISTEN value: • **IP**: the multicast IP address of the group • **Port**: the IP port of the Multicast Paging group. The valid value is an even integer from 1024 to 65535. • **Priority**: the group priority • **Label**: the group label which the phone displays when the incoming page is played
Multicast Paging Groups To Send	If the Multicast Paging feature is enabled, you can add, edit or delete outgoing multicast page groups in this section. The configuration fields are equivalent to the MP_GROUPS_TO_SEND value and control the same settings as Multicast Paging Groups To Send fields. • **IP** • **Port** • **Label**

Related links

Multicast Paging configuration on page 316

Setting Pre-configuration of keys

About this task

Use this procedure to configure a set of pre-determined phone keys for users with the help of the web interface. The pre-configured keys can be used to access features, applications or line appearances.

You can configure pre-determined keys for the phone and button module. The primary display of the device provides the user all 96 keys regardless of any button modules attached. The pre-configured keys corresponding to phone and button module lines are as follows:

- 1 to 24 – phone keys;
- 25 to 48 – button module 1 keys;
- 49 to 72 – button module 2 keys;
- 73 to 96 – button module 3 keys.

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Key Configuration**.
3. On the Key Configuration tab, click one of the following:
   - **Keys**
   - **BM 1 (25–48)**
   - **BM 2 (49–72)**
   - **BM 3 (73–96)**
4. For any key of the selected tab, enter the required value in the following fields:
   - **Type**
   - **Name**
   - **Attribute 1**
   - **Attribute 2**
   - **Label**
5. To clear the key configuration, click the Delete icon on the right.

   If your browser displays the `Confirm Delete Key?` notification, do not select the **Prevent this page from creating additional dialogs** check box. Selecting it disables deleting the key configuration.
6. Click one of the following:
   - **Save**: To save the changes.
   - **Restore customization**: To clear all the key values customized by the user with the help of the phone interface and modified by the administrator through web interface and

revert to the values provided by the server environment and additionally pre-configured in the `46xxsettings.txt` file.

You can modify or delete a forced pre-configured key only in the `46xxsettings.txt` file.

Related links

Pre-configuration of keys on page 221
PHONEKEY parameter values on page 552
Pre-configuration of keys parameter on page 221

Pre-configuration fields

On the Key Configuration tab, the following fields are available for configuring pre-determined keys on the phone and button module.

Name	Description
Key	Displays the list of phone keys that can be configured on the selected tab. The keys corresponding to the tabs are as follows: • Keys – 1 to 24 phone keys; • BM 1 (25–48) – 25 to 48 keys of the first attached button module; • BM 2 (49–72) – 49 to 72 keys of the second attached button module; • BM 3 (73–96) – 73 to 96 keys of the third attached button module.
Type	Contains the types of key configuration. The values are: • Feature • Application • Line • Autodial • Contact • BLF In Asterisk environment, if a value for the BLF type is not set, you can add, edit and delete it.
Name	Displays the values corresponding to the selected type.
Attribute 1	The field is available when the selected type and name of the key require setting this value.
Attribute 2	The field is available when the selected type and name of the key require setting this value.

Table continues…

Name	Description
Label	Adds the key label to the Phone screen or the button module.

Configuring softkey sets

About this task

Use this procedure to configure custom Softkey sets for each call appearance and state.

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Softkey sets**.
3. Select one of the following tabs: **Call Appearance** tab.
4. **(Optional)** If you are using an Open SIP environment, **BLF** and **SCA/BCA/BLA** tabs are enabled and you can select one of them. If you are using Avaya Aura®, these tabs are disabled.
5. In the the selected tab, configure the following states:
   - **Active**
   - **Active Page Target**: this state is available in **SCA** tab.
   - **Idle**
   - **Outgoing**
   - **Incoming Visual**
   - **Incoming**
   - **Dialing**: this state is available in **CA SCA/BCA/BLA** tabs.
   - **Dialtone**: this state is available in **CA SCA/BCA/BLA** tabs.
   - **Transfer Dialing**: this state is available in **CA SCA/BCA/BLA** tabs.
   - **Transfer Outgoing**: this state is available in **CA SCA/BCA/BLA** tabs.
   - **Transfer Consult**: this state is available in **CA SCA/BCA/BLA** tabs.
   - **Conference Dialing** : this state is available in **CA SCA/BCA/BLA** tabs.
   - **Conference Active** : this state is available in **CA SCA/BCA/BLA** tabs.
   - **Conference Outgoing** : this state is available in **CA SCA/BCA/BLA** tabs.
   - **Conference Consult** : this state is available in **CA SCA/BCA/BLA** tabs.
   - **Held**: this state is available in **SCA/BCA/BLA** tab.
   - **Remote Held**: this state is available in **SCA/BCA/BLA** tab.

- **Remote Active**: this state is available in **SCA/BCA/BLA** tab.

6. For each state, configure the following fields for each call appearance:
   - **Type**
   - **Action**
   - **Label**
   - **Override**
   - **Attribute 1**: This field is available only for **Incoming** and **Incoming Visual** states.
7. Click one of the following:
   - **Save**: To save the changes.
   - **Reset to Default**: To revert to the default values.

   You can revert to default values for each state separately, using the **Reset to Default** in each state tab, or for all states at once, using the **Reset to Default** in CA or BLF tab.

Deleting Softkey

About this task

You can remove or delete the softkey.

Before you begin

Ensure that there is at least one softkey configured on the phone to delete it.

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Softkey Sets**.
3. To clear the Softkey configuration, click the Delete icon on the right.

   If your browser displays the **Confirm Delete Key?** notification, do not select the **Don't let this page create more messages** check box. Selecting it disables deleting the key configuration.
4. Do one of the following:
   - Click **Save** to save the changes.
   - Click **Reset to default** to clear all the softkey values and revert to the default values.

Softkey sets field description

Softkey sets Configuration by states:

Name	Description
Active	Opens a separate configuration tab for the Active call state.

Table continues…

Name	Description
Active Page Target	Opens a separate configuration tab for the Active call state.
Idle	Opens a separate configuration tab for the Idle call state.
DND	Opens a separate configuration tab for the DND call state.
Outgoing	Opens a separate configuration tab for the Outgoing call state.
Incoming Visual	Opens a separate configuration tab for the Incoming Visual call state.
Dialing	Opens a separate configuration tab for the Dialing call state.
Dialtone	Opens a separate configuration tab for the Dialtone call state.
Transfer Dialing	Opens a separate configuration tab for the Transfer Dialing call state.
Transfer Outgoing	Opens a separate configuration tab for the Transfer Outgoing call state.
Transfer Consult	Opens a separate configuration tab for the Transfer Consult call state.
Conference Dialing	Opens a separate configuration tab for the Conference Dialing call state.
Conference Active	Opens a separate configuration tab for the Conference Active call state.
Conference Outgoing	Opens a separate configuration tab for the Conference Outgoing call state.
Conference Consult	Opens a separate configuration tab for the Conference Consult call state.
Held	Opens a separate configuration tab for the Held call state.
Remote Held	Opens a separate configuration tab for the Remote Held call state.
Remote Active	Opens a separate configuration tab for the Remote Active call state.

Individual Call states configuration fields for each call appearance:

Name	Description
Type	Select one of the following: • Blank • DTMF • Dial • Function • Feature • Application

Table continues…

Name	Description
Action	If you have selected **Dial** or **DTMF** in the **Type** field, you have a text field. Type a string, using only #,0-9,* symbols. If you enter wrong symbols, the phone displays an error message. If you enter more than 32 symbols, the phone truncates the field value to 32 symbols. If you try to leave the **Action** field empty for **Dial** or **DTMF**, the phone displays an error message. If you have selected **Function** in the **Type** field, you can select between the following functions: • Hold • Transfer • End Call • New Call • Conference • Details • Redirect • Emerg • Clear • Dial • Cancel • Complete • Join • Add • Drop • Decline • Ignore • Resume • Barge in • Pick up Each state has its own set of available functions.
Attribute 1	If you select the Redirect function for Incoming and Incoming Visual states, you can configure Attribute 1. In this field, you can enter a phone number you want to redirect your calls to.

Table continues…

Name	Description
Label	You can configure a custom label in this field. If your label exceeds the length of 8 symbols, the phone truncates it. If your label uses incorrect symbols, the phone displays an error message. If you edit a previously correct label and use incorrect symbols, the phone returns to the previous option.
Override	• Choose `Append to default softkeys` to display default c softkeys. • Choose `Replace all softkeys` to display custom softkeys.

Configuring Shared Lines

About this task

Use this procedure to configure Shared Lines and chose between Shared Call Appearance (SCA), Bridged Lines Appearance (BLA) and Bridged Call Appearance (BCA) modes.

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Shared Lines Configuration**.
3. In the Shared Line Configuration tab, configure the following fields:
   - **Shared Line Mode**
   - **Shared Call Appearances Mode**
   - **Primary Line Type**
   - **Provide Shared Line Config in Settings menu**
   - **Show “Call for” for Primary**
   - **Line Seize Duration**
4. In the Primary Shared Line tab and all additional Shared Line tabs, configure the following fields:
   - **Status**
   - **SIP User ID**
   - **Call Appearances**
   - **Barge In**
   - **Display name**

   You can configure up to 10 lines.

5. In all the additional Shared Line tabs, configure the following additional fields:
   - **Use Primary credentials?**
   - **Authentication User ID**
   - **Authentication Password**
   - **Incoming call indication type**
   - **Indication delay**
6. Click one of the following:
   - **Save**: To save the changes.
   - **Reset to Default**: To revert to the default values.

Shared Lines field description

Shared Line Configuration tab fields:

Name	Description
Shared Line Mode	• Choose `SCA` to enable Shared Call Appearance mode. • Choose `BLA` to enable Bridged Lines Appearance mode. • Choose `BCA` to enable Bridged Call Appearance mode.
Shared Call Appearances Mode	You can select between 1 shared call appearance with Blind Transfer only and 1 shared call appearance with Blind Transfer, Consult Transfer and conference. This setting is available only in BLA mode.
Primary Line Type	You can select between Shared or Private lines.
Shared line settings in user menu	You can configure the phone to allow users to access a fully configurable Shared Lines menu in settings, a read only menu or no menu. This setting is disabled in BLA mode.
Show “Call for” for Primary	You can enable or disable the displaying of ‘Call for’ message on a Primary line for an incoming call.
SCA Line Seize Duration	Select a Line Seize duration time in seconds.

Individual Shared Line configuration fields:

Name	Description
Status	You can enable or disable additional lines.

Table continues…

Name	Description
Call Appearances	• Choose a number from 1 to 8 for Shared Call Appearance mode • For Bridged Lines Appearance mode, this option value is 1 by default and cannot be changed. • Choose a number from 1 to 10 for Bridged Call Appearance mode
Barge In	• Choose `Enabled (default)` for Shared Call Appearance mode. • For Bridged Lines Appearance mode, this option value is disabled.
Display name	Select a Display name for the line.
Use Primary credentials?	You can enable or disable the usage of Primary Credentials.
Authentication User ID	• Type your user ID here for Shared Call Appearance mode. This setting is optional. • Remains blank for Bridged Lines Appearance mode.
Authentication Password	• Type your Password here for Shared Call Appearance mode. • Remains blank for Bridged Lines Appearance mode.
Incoming call indication type	You can select incoming call indication type for each shared line. This setting is not available for the primary line.
Indication delay	Select a value number from 0 to 99 seconds.

Restarting your phone through web interface

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Restart**.
3. In the confirmation window `Phone will restart if the phone is in idle state. Do you want to continue?`, click **OK**.

Resetting the phone to Default

Procedure

1. Log in to the web interface.

2. In the navigation pane, click **Reset to Default**.
3. In the confirmation window `Phone will restart and reset all parameters values to factory default if in idle state. Do you want to continue?`, click **OK**.

Configuring the phone using the settings file

The `46xxsettings.txt` file is used to specify certain system parameters. You can get the `46xxsettings.txt` file from the software distribution package with Product Support Notices from the Avaya support website. For more information, see Downloading and saving the software on page 37.

The downloaded `46xxsettings.txt` file contains the list of supported phone models, explanatory notes, the list of commented parameters, their description and allowed values.

The default `46xxsettings.txt` file contains the parameters distributed into the groups, for example, "Server settings (SIP)".

The requirements for settings file parameters

The following rules should be applied when configuring the phone parameters with the `46xxsettings.txt`:

- Any line that does not begin with "SET", "IF", "GOTO", "#", “ADD” or "GET" is treated as a comment.
- To activate a setting, remove the "##" from the beginning of the line for the required parameter, and change the value to the one appropriate for your environment.
- To include spaces in a value, the entire value must be enclosed in double quotes, as in the following example:

```
SET MYCERTCN "Avaya telephone with MAC address $MACADDR"
```

- Only double quotes (ACSII 34) can be used.

Note:

The unsupported symbols for setting the parameters in the `46xxsettings.txt` file are the following: the left double quotation mark (ASCI 8220) and the right double quotation mark (ASCII 8221).

Related links

Overview of the 46xxsettings.txt file

Configuring SIP Server Settings for the Avaya J179 IP Phone

Contents of the settings file

The settings file can include any of the six types of statements, one per line:

- Tags, which are lines that begin with a single "#" character, followed by a single space character, followed by a text string with no spaces.
- `Goto` commands, of the form `GOTO tag`. `Goto` commands cause the phone to continue interpreting the settings file at the next line after a `# tag` statement. If no such statement exists, the rest of the settings file is ignored.

  Important:

  There must be space character between # and tag.
- Conditionals of the form `IFstring1SEQstring2GOTOtag`. Conditionals cause the `Goto` command to be processed if the value of `string1` exactly matches the value of `string2`. `string1` or `string2` can be defined using a macro: `$GROUP`, `$MACADDR`, `$MODEL` and `$MODEL4`. For example: If `$MODEL4 SEQ J179 GOTO J179_CONFIG`. When Avaya J179 IP Phone encounters this line, it goes to tag `# 179_CONFIG`. When other phones encounter this line, its ignored.
- `SET` commands, of the form `SET` parameter_name value. Invalid values cause the specified value to be ignored for the associated parameter_name so the default or previously administered value is retained. All values must be text strings, if the value itself is numeric, you must place the numeric value inside a pair of quotation marks. For example, `"192.x.y.z"`
- Comments, which are statements with characters "##" in the first column.
- `GET` commands, of the form `GET filename`. The phone attempts to download the file named by `filename`, and if it is successfully obtained, it will be interpreted as an additional settings file, and no additional lines will be interpreted in the original file. If the file cannot be obtained, the phone will continue to interpret the original file.

  Note:

  A `filename` can be a macro: `$GROUP`, `$MACADDR`, `$MODEL`, and `$MODEL4`. For example: `GET $MACADDR.txt`. Avaya J100 Series IP Phones attempts to perform a `GET` of the device `MAC address.txt` such as `c81feaddeeff.txt`.

The Avaya-provided upgrade file includes a line that tells the phones to `GET46xxsettings.txt`. This line cause the phone to use HTTP/HTTPS to attempt to download the file specified in the `GET` command. If the file is obtained, its contents are interpreted as an additional script file. That is how your settings are changed from the default settings. If the file cannot be obtained, the phone continues processing the upgrade script file. Also, if the settings file is successfully obtained but this does not change any settings, the phone continues to use HTTP.

The settings file is under your control and is where you can identify non-default option settings, application-specific parameters, etc. You can download a template for this file from the Avaya support Website.

When Avaya J100 Series IP Phones is in the process of downloading configuration from the provisioning server, the phone does one of the following:

- If the phone is unable to download J100Supgrade.txt file then all previously downloaded configuration is cached.
- If the phone is able to download J100Supgrade.txt file then all previously downloaded configuration is cleared.
  - If the phone is able to download the subsequent `46xxsettings.txt` file then the configuration is re-applied.
  - If the phone is unable to download the subsequent `46xxsettings.txt` file then the previously downloaded configuration is cleared.

Related links

Overview of the 46xxsettings.txt file

Modifying the Settings file

About this task

Use this procedure to modify the `Settings` file to provision the phone configuration parameters. The parameter values stored for the users of a particular phone model do not apply to other phone models, even if the corresponding SIP user is the same. When parameters of the settings file are removed or are not used, they are reset to the default values.

Procedure

1. On the file server, go to the directory of the `Settings` file.
2. Open the `Settings` file in a text editor.
3. Set the values of the parameters that you want to provision.
4. Save the `Settings` file.

Result

On the next poll, the phones download the `Settings` file and apply the configuration settings.

Phone display language

By default, the phone display information is in English. Administrators can specify more than four languages for each phone to replace English. Users can then select the display language on the phone.

The user can change the language of the phone and choose one of the following languages:

- Arabic
- Dutch
- English

- French (Canada)
- French (France)
- German
- Hebrew
- Italian
- Japanese
- Korean
- Polish
- Portuguese (Brazil)
- Russian
- Simplified Chinese
- Spanish (Latin America)
- Spanish (Spain)
- Thai
- Traditional Chinese
- Turkish

The actual character input method does not depend on the languages available from the software download. If the phone does not support a character input method, use ASCII.

Note:

Traditional Chinese is supported only for J169/179 SIP IP Phones.

Avaya J129 IP Phone does not support Arabic and Thai languages.

. The downloadable language files contain all the information required for the phone to present the language as part of the user interface.

Use `46xxsettings.txt` file to customize the language of the phone.

- SYSTEM_LANGUAGE- Contains the name of the default system language file used in the phone. The file name must be one of the files listed in the LANGUAGES parameter. If no file name is specified, or if the file name does not match with one of the LANGUAGES values, the phone uses its built-in English text strings. File name must end in .xml
- LANGUAGES- Specifies the language files to be installed or downloaded to the phone. File names may be full URL, relative path name, or file name. (0 to 1096 ASCII characters, including commas). File names must end in .xml. For example, to indicate that and Russian, Parisian French, Latin American Spanish, and Korean are the available languages, the setting is **`SET LANGUAGES Mlf_Russian.xml,Mlf_ParisianFrench.xml,Mlf_LatinAmericanSpanish.xml, Mlf_Korean.xml`**
- LANG0STAT- Allows the user to select the built-in English language when other languages are downloaded. If LANG0STAT is "0" and at least one language is downloaded, the user cannot select the built-in English language. If LANG0STAT is "1" (the default) the user can select the built-in English language text strings.

To download a language file or to review pertinent information, go to the Avaya Support website.

Pre-configuration of keys

With the Pre-configuration of keys feature, you can configure a set of phone keys at specific line locations on the phone screen for accessing features, applications or line appearances. You can also add BLF lines and autodials with this feature. The configured keys can be labelled as required.

Pre-configuration of keys is configured per user or a group of users, and it is applied to all the phones used by that user or group.

The line types, for example, features and BLFs are pre-determined by a server environment you use. You can configure forced or non-forced values for the PHONEKEY parameter. If you select a forced value, the user is not able to modify it using the phone interface, and the administrator can modify it only in the `46xxsettings.txt` file. If the phone key configuration is not forced, the user can change key mapping and labels as required, and these changes override the configuration set by the system administrator.

The Pre-configuration of keys feature can be configured in either of the following ways:

- by setting the PHONEKEY parameter in the `46xxsettings.txt` file.
- by adding the pre-configured keys in the web interface.

Related links

Phone configuration on page 93
Pre-configuration of keys parameter on page 221
Phonekey Labels on page 223
Viewing PHONEKEYLIST parameter details on page 223
Setting Pre-configuration of keys on page 207
PHONEKEY parameter values on page 552
Pre-configuration of keys parameter on page 221

Pre-configuration of keys parameter

The Pre-configuration of keys feature can be administered by setting the PHONEKEY parameter in the `46xxsettings.txt` file. Using this parameter an administrator can:

- Place a specific line in a line key location
- Provide a label for this line
- Specify if a user can move or relable this line

This parameter is used for mapping the feature, application, call appearance and autodial keys available in the Phone screen. All the PHONEKEY values and keywords are case-insensitive except values set in `Label`.

The PHONEKEY parameter should be set in the following format without any intervening spaces before and after the equality sign (“=”):

```
SET PHONEKEY "Key=[n1];Type=[Feature|Application|Line|
Autodial];Name=[name];attr1=[value];attr2=[value];Label=[label (optional)][;Forced
(optional)]"
```

where:

- `[n1]` corresponds to the number of the phone key to be configured. The allowed values are positive integers from 1 to 96.
- `[Feature|Application|Line|Autodial]` corresponds to the functionality to be assigned to a key. The allowed values are: `feature`, `application` , `line` or `autodial`.
- `[name]`, depending on the functionality entered in `Type`, can be either of the following:
  - the name of the feature that will be accessed by pressing the customized phone key, e.g., `callfwd` (Call Forward), `blf` (Busy Lamp Field), etc.
  - the name of the application, e.g., `lock`, `logout`, `screensaver`, etc.
  - the type of the phone line that will be accessed. The allowed values are: `primary`, `sca` (Shared Call Appearance).
  - Phone extension number for autodial.
- `[label]` is the key label that will be displayed on the Phone screen. This setting is optional and case-sensitive.

  You can configure `Label` through the `46xxsettings.txt` file and through the Web Interface in the Key Configuration tab. The `46xxsettings.txt` is the preferable way of configuring labels.
- `Forced` determines whether the user can move, delete, or relabel a key. This setting is optional.

  There are several main scenarios for the `Forced` and `Non-forced`settings:

  An occupied location referred below is a location that is already configured for a line type on the phone. An empty location referred below is an unconfigured key location.
  - If `Forced` is set and the key location is empty, the key definition is applied.
  - If `Forced` is set for an occupied key location, it overrides the existing key or moves the occupied key to a different location closer to the defined location. If no empty location is available, a contact or an application line key is overridden. If no contact or application line key is available, the new definition is dropped.
  - If `Forced` is not set and the location is empty, the new definition is applied.
  - If `Forced` is not set and the location is already occupied, the new definition is applied to an empty location closer to the defined location. If no empty location is available a contact or an application line key is overridden. If no contact or application line key is available, the new definition is dropped.

Related links

Pre-configuration of keys on page 221
Setting Pre-configuration of keys on page 207
Pre-configuration of keys on page 221

PHONEKEY parameter values on page 552

Phonekey Labels

In the 3PCC environment, you can configure Label values for the PHONEKEY parameter using the web user interface or `46xxsettings.txt` file.

Labels that you configure using the web user interface can be modified by a user. Labels that you configure using the `46xxsettings.txt` file for Forced cannot be user-modified, they can be modified only by an Administrator in the `46xxsettings.txt`.

The labels that you configure using the `46xxsettings.txt` file for non-forced key can be modified from web user interface or on the phone.

If there are no labels configured for a line key by the administrator or the user, the phone provides a default label automatically.

When the phone looks for a lable to use, it uses the following priority:

- User-modified labels
- Administrator-set labels
- Default labels

When you add several labels for a single line key, the phone uses only the last one. The phone only takes one administrator-defined label for each entity or same feature.

Starting with 4.0.4, `[label]` allows users to add non-Latin symbols to their customized labels if their native language uses an alphabet other than Latin. Both left to right (LTR) and right to left (RTL) languages are supported. For example:

```
SET PHONEKEY "Key=6;Type=autodial;Name=autodial;Attr1=123456;Label=АБВГДЕЁЖЗ"
```

where `Label` defines additional non-Latin and extended Latin symbols that can be used when editing custom labels on the phone. You can add up to 31 symbols. The web interface has left alignment, but you can copy a label text in RTL language from clipboard to the `label` input line. The phone displays RTL labels in the left to right mode.

Note:

Encoding other than ANSI must be used for the `46xxsettings.txt` to store non-Latin symbols correctly.

Related links

Pre-configuration of keys on page 221

Viewing PHONEKEYLIST parameter details

About this task

Use this task to view the PHONEKEYLIST parameter value in the MIB browser application.

When the phone downloads the `46xxsettings.txt` file, the settings for the PHONEKEY parameter are parsed and stored in the PHONE_KEY_LIST_ENHANCED parameter.

PHONE_KEY_LIST_ENHANCED is an internal parameter but you can view its value in a SNMP table of the MIB browser application.

Before you begin

- Ensure the MIB browser application is installed on your local computer.
- Obtain the IP address of the phone.

Procedure

1. Open your MIB browser application.
2. Navigate to **File** > **Load MIBs** to upload the required `.mib` file. The `.mib` file is a part of the firmware package.
3. In the **Address** field, enter the IP address of the phone.
4. In the **SNMP MIBs** list, double-click the PHONEKEYLIST parameter to view its value.

   The MIB browser application displays the parameter value in **Result Table** on the right, in the **Name**, **Value** and **Type** columns.

Related links

Pre-configuration of keys on page 221
Viewing IP address of the phone on page 117

Soft key configuration

You can configure soft keys for various call appearances to activate in-call features. Users use these soft keys during a call, instead of entering digital codes.

You can create new soft keys with the default soft keys or replace the existing soft keys for the following call appearance states:

Primary appearance states:

- Active
- Active Page Target
- Idle
- Incoming
- Incoming visual
- Incoming ignore
- Held
- Outgoing
- Transfer

- Transfer Outgoing
- Transfer Dialing
- Transfer Consult
- Conference
- Conference Outgoing
- Conference Dialing
- Conference Consult
- Conference Active
- Dialtone
- Dialing

BLF and BLF Park call appearance states:

- Active
- Idle
- Incoming
- Incoming visual
- Outgoing

BLA and BCA call appearance states:

- Active
- Idle
- Incoming
- Incoming visual
- Outgoing
- Transfer
- Transfer Outgoing
- Transfer Dialing
- Transfer Consult
- Conference
- Conference Outgoing
- Conference Dialing
- Conference Consult
- Conference Active
- Dialing
- Dialtone
- Remote Active

- Remote Held

Note:

The call appearance state incoming visual is the incoming call pop-up, which the phone screen displays when a call initially appears on the phone.

In the call appearance state incoming, the phone's main home screen displays call alerting if the user doesn't answer the call immediately.

You can configure the soft keys using the phone web Interface or the `46xxsettings.txt` file. You can configure up to 12 soft keys for each call appearance state. If you add more than 12 soft keys using the `46xxsettings.txt` file, the first 12 soft keys are available for the users.

The set of in-call features and digital codes to activate these features depends on the server environment.

Related links

Phone configuration on page 93
Configuration of soft key parameter for primary call appearance state on page 226
Configuration of soft key parameters for Shared Call Appearance and Bridged Line Appearance states on page 235
Configuration of soft key parameter for Busy lamp field call appearance states on page 245

Configuration of soft key parameter for primary call appearance state

You can configure the following parameters using the `46xxsettings.txt` file:

Use the **ADD** command to configure up to 12 soft keys in the `46xxsettings.txt` file. If you use several **SET** commands, the latest one overrides the previous one.

Following are the details of allowed values in the soft key parameter values:

Name	Default	Description

SOFTKEY_ACTIVE	Null	Specifies the custom soft key for the call appearance lines in an Active state. You can provide the soft key attributes and labels, which a phone displays during an active call, along with standard active call soft keys.
		For example:
		`SET SOFTKEY_ACTIVE "type=dtmf;action=##*3;label=Park"`
		`ADD SOFTKEY_ACTIVE "type=dtmf;action=*34;label=Record"`

Table continues…

Name	Default	Description

SOFTKEY_ACTIVE_PAGETARGET	Null	Specifies the custom soft key for the call appearance lines in an Active Page target state. You can provide the soft key attributes and labels, which a phone displays during a page call, along with standard soft keys.
		For example:
		`SET SOFTKEY_ACTIVE_PAGETARGET "type=dtmf;action=AnswerDigitSequence;label=Answer"`
		`ADD SOFTKEY_ACTIVE_PAGETARGET "type=function;action=endcall;label=End"`

SOFTKEY_IDLE	Null	Specifies the custom soft key for the call appearance lines in an Idle state. You can provide the soft key attributes and labels, which a phone displays during idle, along with standard soft keys.
		For example:
		`SET SOFTKEY_IDLE "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_IDLE "type=function;action=emergency;label=emergency2"`

SOFTKEY_INCOMING	Null	Specifies the custom soft key for the call appearance lines in an Incoming state. You can provide the soft key attributes and labels, which a phone displays during an incoming call, along with standard soft keys.
		For example:
		`SET SOFTKEY_INCOMING "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_INCOMING "type=function;action=decline;label=reject"`

Table continues…

Name	Default	Description

SOFTKEY_INCOMING_VISUAL	Null	Specifies the custom soft key for the call appearance lines in an Incoming Visual state. You can provide the soft key attributes and labels, which a phone displays during an incoming call, along with standard soft keys.
		For example:
		`SET SOFTKEY_INCOMING_VISUAL "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_INCOMING_VISUAL "type=function;action=redirect;attr1=65324;label=divert"`

SOFTKEY_OUTGOING	Null	Specifies the custom soft key for the call appearance lines in an Outgoing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_OUTGOING "type=function;action=endcall;label=call"`
		`ADD SOFTKEY_OUTGOING "type=function;action=endcall;label=call"`

SOFTKEY_HELD	Null	Specifies the custom soft key for the call appearance lines in a Held state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_HELD "type=function;action=newcall;label=hold"`
		`ADD SOFTKEY_HELD "type=function;action=resume;label=drop"`

Table continues…

Name	Default	Description

SOFTKEY_DIALING	Null	Specifies the custom soft key for the call appearance lines in an Dialing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_DIALING "type=function;action=redial;label=dial"`
		`ADD SOFTKEY_DIALING "type=function;action=endcall;label=finish"`

SOFTKEY_DIALTONE	Null	Specifies the custom soft key for the call appearance lines in a Dialtone state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_DIALTONE "type=function;action=redial;label=dial"`
		`ADD SOFTKEY_DIALTONE "type=function;action=endcall;label=finish"`

SOFTKEY_CONFERENCE_DIALING	Null	Specifies the custom soft key for the call appearance lines in a Conference Dialing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_CONFERENCE_DIALING "type=function;action=clear;label=drop"`
		`ADD SOFTKEY_CONFERENCE_DIALING "type=function;action=endcall;label=finish"`

Table continues…

Name	Default	Description

SOFTKEY_CONFERENCE_OUTGOING	Null	Specifies the custom soft key for the call appearance lines in a Conference Outgoing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_CONFERENCE_OUTGOING "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_CONFERENCE_OUTGOING "type=function;action=clear;label=finish"`

SOFTKEY_CONFERENCE_CONSULT	Null	Specifies the custom soft key for the call appearance lines in a Conference Consult state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_CONFERENCE_CONSULT "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_CONFERENCE_CONSULT "type=function;action=endcall;label=finish"`

Table continues…

Name	Default	Description

SOFTKEY_CONFERENCE_ACTIVE	Null	Specifies the custom soft key for the call appearance lines in a Conference Active state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_CONFERENCE_ACTIVE "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_CONFERENCE_ACTIVE "type=function;action=endcall;label=finish"`

SOFTKEY_TRANSFER_DIALING	Null	Specifies the custom soft key for the call appearance lines in a Transfer Dialing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_TRANSFER_DIALING "type=function;action=clear;label=drop"`
		`ADD SOFTKEY_TRANSFER_DIALING "type=function;action=endcall;label=finish"`

Table continues…

Name	Default	Description

SOFTKEY_TRANSFER_OUTGOING	Null	Specifies the custom soft key for the call appearance lines in a Transfer Outgoing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_TRANSFER_OUTGOING "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_TRANSFER_OUTGOING "type=function;action=clear;label=finish"`

SOFTKEY_TRANSFER_CONSULT	Null	Specifies the custom soft key for the call appearance lines in a Transfer Consult state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_TRANSFER_CONSULT "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_TRANSFER_CONSULT "type=function;action=endcall;label=finish"`

OVERRIDE_SOFTKEY_IDLE	0	Specifies if the phone shows default softkeys for CA lines in an IDLE state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_ACTIVE	0	Specifies if the phone shows default softkeys for CA lines in an ACTIVE state. Value operation: • 0: No • 1: Yes

Table continues…

Name	Default	Description
OVERRIDE_SOFTKEY_INCOMING	0	Specifies if the phone shows default softkeys for CA lines in an INCOMING state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_INCOMING_VISUAL	0	Specifies if the phone shows default softkeys for CA lines in an INCOMING_VISUAL state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_OUTGOING	0	Specifies if the phone shows default softkeys for CA lines in an OUTGOING state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_HELD	0	Specifies if the phone shows default softkeys for CA lines in a HELD state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_DIALING	0	Specifies if the phone shows default softkeys for CA lines in a Dialing state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_DIALTONE	0	Specifies if the phone shows default softkeys for CA lines in an Dialtone state. Value operation: • 0: No • 1: Yes

Table continues…

Name	Default	Description
OVERRIDE_SOFTKEY_CONFERENCE_DIALING	0	Specifies if the phone shows default softkeys for CA lines in an Conference Dialing state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_CONFERENCE_OUTGOING	0	Specifies if the phone shows default softkeys for CA lines in an Conference Outgoing state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_CONFERENCE_CONSULT	0	Specifies if the phone shows default softkeys for CA lines in an Conference Consult state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_CONFERENCE_ACTIVE	0	Specifies if the phone shows default softkeys for CA lines in an Conference Active state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_TRANSFER_DIALING	0	Specifies if the phone shows default softkeys for CA lines in an Transfer Dialing state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_TRANSFER_OUTGOING	0	Specifies if the phone shows default softkeys for CA lines in an Transfer Outgoing state. Value operation: • 0: No • 1: Yes

Table continues…

Name	Default	Description
OVERRIDE_SOFTKEY_TRANSFER_CONSULT	0	Specifies if the phone shows default softkeys for CA lines in an Transfer Consult state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_ACTIVE_PAGETARGET	0	Specifies if the phone shows default softkeys for CA lines in an ACTIVE_PAGE state. Value operation: • 0: No • 1: Yes

Related links

Soft key configuration on page 224
Soft key parameter values on page 546

Configuration of soft key parameters for Shared Call Appearance and Bridged Line Appearance states

You can configure the following parameters using the `46xxsettings.txt` file:

Use the **ADD** command to configure up to 12 soft keys in the `46xxsettings.txt` file. If you use several **SET** commands, the latest one overrides the previous one.

Following are the details of allowed values in the soft key parameter values:

Name	Default	Description

SOFTKEY_SCA_ACTIVE	Null	Specifies the custom soft key for the shared lines in an Active state. You can provide the soft key attributes and labels, which a phone displays during an active call, along with standard active call soft keys.
		For example:
		`SET SOFTKEY_SCA_ACTIVE "type=dtmf;action=##*3;label=Park"`
		`ADD SOFTKEY_SCA_ACTIVE "type=dtmf;action=*34;label=Record"`

Table continues…

Name	Default	Description

SOFTKEY_SCA_IDLE	Null	Specifies the custom soft key for the shared lines in an Idle state. You can provide the soft key attributes and labels, which a phone displays during idle, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_IDLE "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_SCA_IDLE "type=function;action=emergency;label=emergency2"`

SOFTKEY_SCA_INCOMING	Null	Specifies the custom soft key for the shared lines in an Incoming state. You can provide the soft key attributes and labels, which a phone displays during an incoming call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_INCOMING "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_SCA_INCOMING "type=function;action=decline;label=reject"`

SOFTKEY_SCA_INCOMING_VISUAL	Null	Specifies the custom soft key for the shared lines in an Incoming Visual state. You can provide the soft key attributes and labels, which a phone displays during an incoming call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_INCOMING_VISUAL "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_SCA_INCOMING_VISUAL "type=function;action=redirect;attr1=65324;label=divert"`

Table continues…

Name	Default	Description

SOFTKEY_SCA_OUTGOING	Null	Specifies the custom soft key for the shared lines in an Outgoing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_OUTGOING "type=function;action=endcall;label=drop"`
		`ADD SOFTKEY_SCA_OUTGOING "type=function;action=endcall;label=finish"`

SOFTKEY_SCA_HELD	Null	Specifies the custom soft key for the shared lines in a Held state. You can provide the soft key attributes and labels, which a phone displays during an incoming call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_HELD "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_SCA_HELD "type=function;action=redirect;attr1=65324;label=redirect"`

SOFTKEY_SCA_REMOTE_ACTIVE	Null	Specifies the custom soft key for the shared lines in a Remote Active state. You can provide the soft key attributes and labels, which a phone displays during an incoming call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_REMOTE_ACTIVE "type=function;action=barge in;label=barge in"`
		`ADD SOFTKEY_SCA_REMOTE_ACTIVE "type=function;action=newcall;label=call"`

Table continues…

Name	Default	Description

SOFTKEY_SCA_REMOTE_HELD	Null	Specifies the custom soft key for the shared lines in a Remote Held state. You can provide the soft key attributes and labels, which a phone displays during an incoming call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_REMOTE_HELD "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_SCA_REMOTE_HELD "type=function;action=pickup;label=answer"`

SOFTKEY_SCA_DIALING	Null	Specifies the custom soft key for the shared lines in an Dialing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_DIALING "type=function;action=redial;label=dial"`
		`ADD SOFTKEY_SCA_DIALING "type=function;action=endcall;label=finish"`

SOFTKEY_SCA_DIALTONE	Null	Specifies the custom soft key for the shared lines in a Dialtone state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_HELD "type=function;action=redial;label=dial"`
		`ADD SOFTKEY_HELD "type=function;action=endcall;label=finish"`

Table continues…

Name	Default	Description

SOFTKEY_SCA_CONFERENCE_DIALING	Null	Specifies the custom soft key for the shared lines in a Conference Dialing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_CONFERENCE_DIALING "type=function;action=clear;label=drop"`
		`ADD SOFTKEY_SCA_CONFERENCE_DIALING "type=function;action=endcall;label=finish"`

SOFTKEY_SCA_CONFERENCE_OUTGOING	Null	Specifies the custom soft key for the shared lines in a Conference Outgoing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_CONFERENCE_OUTGOING "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_SCA_CONFERENCE_OUTGOING "type=function;action=clear;label=finish"`

Table continues…

Name	Default	Description

SOFTKEY_SCA_CONFERENCE_CONSULT	Null	Specifies the custom soft key for the shared lines in a Conference Consult state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_CONFERENCE_CONSULT "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_SCA_CONFERENCE_CONSULT "type=function;action=endcall;label=finish"`

SOFTKEY_SCA_CONFERENCE_ACTIVE	Null	Specifies the custom soft key for the shared lines in a Conference Active state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_CONFERENCE_ACTIVE "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_SCA_CONFERENCE_ACTIVE "type=function;action=endcall;label=finish"`

Table continues…

Name	Default	Description

SOFTKEY_SCA_TRANSFER_DIALING	Null	Specifies the custom soft key for the shared lines in a Transfer Dialing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_TRANSFER_DIALING "type=function;action=clear;label=drop"`
		`ADD SOFTKEY_SCA_TRANSFER_DIALING "type=function;action=endcall;label=finish"`

SOFTKEY_SCA_TRANSFER_OUTGOING	Null	Specifies the custom soft key for the shared lines in a Transfer Outgoing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_TRANSFER_OUTGOING "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_SCA_TRANSFER_OUTGOING "type=function;action=clear;label=finish"`

Table continues…

Name	Default	Description

SOFTKEY_SCA_TRANSFER_CONSULT	Null	Specifies the custom soft key for the shared lines in a Transfer Consult state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_TRANSFER_CONSULT "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_SCA_TRANSFER_CONSULT "type=function;action=endcall;label=finish"`

OVERRIDE_SOFTKEY_SCA_IDLE	0	Specifies if the phone shows default soft keys for shared lines in an Idle state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_ACTIVE	0	Specifies if the phone shows default soft keys for shared lines in an Active state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_INCOMING	0	Specifies if the phone shows default soft keys for shared lines in an Incoming state. Value operation: • 0: No • 1: Yes

Table continues…

Name	Default	Description
OVERRIDE_SOFTKEY_SCA_INCOMING_VISUAL	0	Specifies if the phone shows default soft keys for shared lines in an Incoming Visual state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_OUTGOING	0	Specifies if the phone shows default soft keys for shared lines in an Outgoing state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_HELD	0	Specifies if the phone shows default soft keys for shared lines in a Held state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_REMOTE_ACTIVE	0	Specifies if the phone shows default soft keys for shared lines in a Remote Active state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_REMOTE_ HELD	0	Specifies if the phone shows default soft keys for shared lines in a Remote Held state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_DIALING	0	Specifies if the phone shows default soft keys for shared lines in an Dialing state. Value operation: • 0: No • 1: Yes

Table continues…

Name	Default	Description
OVERRIDE_SOFTKEY_SCA_DIALTONE	0	Specifies if the phone shows default soft keys for shared lines in an Dialtone state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_CONFERENCE_DIALING	0	Specifies if the phone shows default softkeys for shared lines in an Conference Dialing state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_CONFERENCE_OUTGOING	0	Specifies if the phone shows default softkeys for shared lines in an Conference Outgoing state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_CONFERENCE_CONSULT	0	Specifies if the phone shows default softkeys for shared lines in an Conference Consult state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_CONFERENCE_ACTIVE	0	Specifies if the phone shows default softkeys for shared lines in an Conference Consult state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_TRANSFER_DIALING	0	Specifies if the phone shows default soft keys for shared lines in an Transfer Dialing state. Value operation: • 0: No • 1: Yes

Table continues…

Name	Default	Description
OVERRIDE_SOFTKEY_SCA_TRANSFER_OUTGOING	0	Specifies if the phone shows default soft keys for shared lines in an Transfer Outgoing state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_TRANSFER_CONSULT	0	Specifies if the phone shows default soft keys for shared lines in an Transfer Consult state. Value operation: • 0: No • 1: Yes

Related links

Soft key configuration on page 224

Configuration of soft key parameter for Busy lamp field call appearance states

You can configure the following parameters using the `46xxsettings.txt` file:

Use the **ADD** command to configure up to 12 soft keys in the `46xxsettings.txt` file. If you use several **SET** commands, the latest one overrides the previous one.

See the details of allowed values in the Soft key parameter values.

Note:

This feature is available on Avaya J139 IP Phone, Avaya J159 IP Phone, Avaya J169/J179 IP Phone, and Avaya J189 IP Phones.

Name	Default	Description

SOFTKEY_BLF_ACTIVE	Null	Specifies the custom soft key for the call appearance lines in BLF Active state. You can provide the soft key attributes and labels, which a phone displays during an active BLF call, along with to standard active call soft keys.
		For example:
		`SET SOFTKEY_BLF_ACTIVE "type=dial;action=*80$attr2;label=dial"`
		`ADD SOFTKEY_BLF_ACTIVE "type=function;action=call;label=call"`

SOFTKEY_BLF_DND	Null	Specifies the custom soft key for the call appearance lines in BLF DND state. You can provide the soft key attributes and labels, which a phone displays during an active BLF call, along with to standard active call soft keys. For example: `ADD SOFTKEY_BLF_DND "type=function;action=ignore;label=ignore"`

SOFTKEY_BLF_IDLE	Null	Specifies the custom soft key for the call appearance lines in BLF Idle state. You can provide the soft key attributes and labels which a phone displays during idle BLF line, along with standard soft keys.
		For example:
		`SET SOFTKEY_BLF_IDLE "type=function;action=call;label=call"`
		`ADD SOFTKEY_BLF_IDLE "type=function;action=pickup;label=pickup"`

Table continues…

Name	Default	Description

SOFTKEY_BLF_INCOMING	Null	Specifies the custom soft key for the call appearance lines in BLF Incoming state. You can provide the soft key attributes and labels, which a phone displays during an incoming BLF call, along with standard soft keys.
		For example:
		`SET SOFTKEY_BLF_INCOMING "type=function;action=call;label=call"`
		`ADD SOFTKEY_BLF_INCOMING "type=function;action=bargein;label=Bargein"`

SOFTKEY_BLF_INCOMING_VISUAL	Null	Specifies the custom soft key for the call appearance lines in BLF Incoming Visual state. You can provide the soft key attributes and labels, which a phone displays during an incoming BLF call, along with standard soft keys.
		For example:
		`SET SOFTKEY_BLF_INCOMING_VISUAL "type=function;action=pickup;label=Pickup"`
		`ADD SOFTKEY_BLF_INCOMING_VISUAL "type=function;action=ignore;label=reject"`

SOFTKEY_BLF_OUTGOING	Null	Specifies the custom soft key for the call appearance lines in BLF outgoing state. You can provide the soft key attributes and labels, which a phone displays during a outgoing BLF call, along with addition standard soft keys.
		For example:
		`SET SOFTKEY_BLF_OUTGOING "type=dial;action=*80$attr2;label=dial"`
		`ADD SOFTKEY_BLF_OUTGOING "type=function;action=call;label=call"`

Table continues…

Name	Default	Description
OVERRIDE_SOFTKEY_BLF_IDLE	0	Specifies if the phone shows default softkeys for BLF lines in an IDLE state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_BLF_ACTIVE	0	Specifies if the phone shows default softkeys for BLF lines in an ACTIVE state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_BLF_DND	0	Specifies if the phone shows default softkeys for BLF lines in an DND state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_BLF_INCOMING	0	Specifies if the phone shows default softkeys for BLF lines in an ALERTING state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_BLF_INCOMING_VISUAL	0	Specifies if the phone shows default softkeys for BLF lines in an ALERTING state on the incoming call view. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_BLF_OUTGOING	0	Specifies if the phone shows default softkeys for BLF lines in the OUTGOING_RING state. Value operation: • 0: No • 1: Yes

Related links

Soft key configuration on page 224
Soft key parameter values on page 546

Chapter 7: Feature and application configuration

You can configure basic and advanced telephony features for the phone users. The features can be configured locally, or on the telephony feature server. In addition, the phone provides applications that you can configure for the users.

The features that are currently configured are listed in the Feature screen. The applications that are currently configured are listed in the Applications screen. You must configure the related parameters to activate these feature for users.

The following tables list the applications and features, their description, and the corresponding topics.

Application name	Description	Reference
Calendar	To access Microsoft® Exchange Server calendar.	Calendar on page 252
Contacts	To manage your contacts list.	Contacts list on page 254
Recents	To manage your call history.	Recents on page 256

Feature name	Description	Reference
Active call shortcut keys	To use Busy Lamp Fields, Autodial, or Contacts keys as shortcuts to perform a specific action during an active or a held call.	Active call shortcut keys on page 262
Anywhere and Mobility	To make and receive calls using any phone from any location.	Anywhere and Mobility on page 265
Avaya Spaces	To use Avaya Spaces application through the Calendar.	Avaya Spaces Calendar integration on page 266
BroadWorks Directory	To manage directory in the BroadWorks environment.	BroadWorks Directory on page 279
BroadSoft XSI	To integrate telephony applications with BroadWorks servers.	BroadSoft XSI support on page 269
Busy Lamp Field	To monitor the status of other phones connected to the same network and manage call operations on their behalf.	Busy Lamp Field on page 271

Table continues…

Feature name	Description	Reference
Call Forward	To divert incoming calls to another phone extension.	Call forwarding on a generic SIP server on page 288
Call Park	To park an active call and resume the call from any other phone in the organization.	Call Park on page 288
Call Waiting	To enable a notification for the another incoming call, when you are on a call.	Call Waiting on page 291
Distinctive ringing	To use different call ringtone for group calls.	Distinctive Ringing on page 298
Distinctive alert waiting tone	To use distinctive ringtone for call waiting service.	Distinctive Alert Waiting Tone on page 298
Downloadable directory	To upload or update the global contacts using the .xml file.	Downloadable directory on page 296
Flexible Seating	To log in to the phone extension from another phone.	Flexible Seating on page 304
Group Paging	To use paging for a group of users.	Group Paging on page 305
LDAP Directory	To search global contacts through an LDAP server.	LDAP Directory on page 306
Long-term acoustic protection	To protect the headset user's hearing.	Long-term acoustic protection on page 305
Multicast Paging	To send a multicast page to a group of phones.	Multicast Paging on page 315
Pre-configuration of keys	To configure a set of phone keys for accessing features, applications or line appearances.	Pre-configuration of keys on page 221
Prioritization of codecs	To set priority of use for all codecs.	Prioritization of codecs on page 318
Phone screen width	To set the default screen width for the phone.	Phone screen width on page 322
Push	To allow trusted applications to send their content to the phone.	Push on page 319
Push-To-Talk	To use automatic call answer.	Push-To-Talk on page 321
Server-initiated update	To update the phone firmware with new settings.	Server-initiated Update on page 335
Shared Call Appearance	To share the phone line with multiple phones to make and receive calls.	Shared Lines on page 324
Shared Parking	To park an active call to a shared phone extension.	Shared Parking on page 333

Table continues…

Feature name	Description	Reference
Simultaneous Ring Personal	To receive calls to additional phone numbers or SIP-URI addresses apart from the primary phone.	Simultaneous Ring Personal on page 336
Voicemail	To listen to your voice mail messages.	Voicemail on page 342
WML browser	To view pre-configured WML pages from the phone menu.	WML browser on page 340

Application configuration

Calendar

The Calendar feature is used to access Microsoft® Exchange Server calendar on the phone. It displays reminders for meetings or appointments on the phone screen.

When Exchange Calendar is active, appointments are displayed in the order of their start times and are removed after the meeting time expires. Calendar information is updated whenever the user log in to the phone.

Calendar configuration

Use `46xxsettings.txt` file to set the following parameters:

Parameter name	Default Value	Description
ENABLE_EXCHANGE_REMINDER	0	Specifies whether or not exchange reminders will be displayed. Value operation: • 0: Not displayed • 1: Displayed **Note:** Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default Value	Description
EXCHANGE_SNOOZE_TIME	5	Specifies the number of minutes in which a reminder must be displayed again after it is temporarily dismissed. Valid values are 0 through 60. **Note:** Avaya J129 IP Phone does not support this feature.
EXCHANGE_AUTH_USERNAME_FORMAT	0	Specifies the necessary format of the username for http authentication. Value operation: • 0: Office 2003/Office2016 username format. Username= <ExchangeUserDomain \ExchangeUserAccount> or Username= <ExchangeUserAccount> if <ExchangeUserDomain> is empty. • 1: Office 365 format. Username= <ExchangeUserAccount@ExchangeUser Domain> or Username= <ExchangeUserAccount> if <ExchangeUserDomain> is empty.
EXCHANGE_REMINDER_TIME	5	Specifies the number of minutes before an appointment at which a reminder will be displayed. Valid values are 0 through 60.
EXCHANGE_REMINDER_TONE	1	Specifies whether or not a tone will be generated the first time an Exchange reminder is displayed. Value operation: • 0: Tone not generated. • 1: Tone generated.
EXCHANGE_USER_DOMAIN	Null	Specifies the domain for the URL used to obtain Exchange contacts and calendar data. The parameter is used as a part of the user authentication. The value can contain 0 to 255 characters.

Table continues…

Parameter name	Default Value	Description
PROVIDE_EXCHANGE_CALENDAR	1	Specifies if menu items for exchange calendar are displayed. Value operation: • 0: Not displayed • 1: Displayed (default)
PROVIDE_EXCHANGE_CONTACTS	1	Specifies if menu items for exchange contacts are displayed. Value operation: • 0: Not displayed • 1: Displayed (default)
USE_EXCHANGE_CALENDAR	0	Specifies whether the Calendar synchronizes with the Microsoft Exchange. Value operation: • 0: To disable synchronization. • 1: To enable synchronization.

Contacts list

With the Contacts application, users can manage their phone contacts list and use the list to make calls. Users can view and edit their contacts and select a contact name or number to make calls. Users can also create and update contact groups with the entries available in the Contacts list and search for users in an LDAP directory.

Following are the types of contacts:

- Local contacts: Contacts the user adds. These contacts are saved as part of the user data.
- System contacts: Entries in a company directory or database.
- Global Exchange contacts: Entries in a company exchange directory.
- Personal Exchange contacts: Contacts from a user exchange account.
- Microsoft® Exchange contacts: Accessible if Microsoft® Exchange is configured.

Contacts list configuration

Use the `46xxsettings.txt` file to set the following parameters:

Parameter name	Default value	Description
ENABLE_CONTACTS	1	Specifies if the contacts application and associated menus are available on the phone. Value Operation: • 0: No. The phone disables the **Contacts** option on the interface • 1: Yes **Note:** The parameter is set to 1 in IP Office 10.1 or later. In previous releases it is set to 0. Set this parameter to 0 to keep the user's data private by default before the user accesses the phone.
ENABLE_MODIFY_CONTACTS		Specifies if the list of contacts and the function of the contacts application can be modified on the phone. Value Operation: • 0: No • 1: Yes
USER_STORE_URI		Specifies the URI path of HTTP/HTTPS server for storing user data.

Configuring Groups list using the web interface

Before you begin

Ensure that you have the Group Number for the user group you add.

Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **Settings**.
3. In **Group Number**, type the group numbers. The value must be between 0 and 999.

Recents

The Recents application presents a log of the last 100 calls on the phone. Each record in the call log contains a call-type icon, the number or the name, and the time-stamp of the call. From the call log, users can do the following:

- View the call history details
- Place a call
- Delete a call record
- Clear the Recents list
- Add a contact

Call log

Depending upon the call type, the call log provides the following information about the last hundred calls on the phone:

- Caller name
- Caller number
- Call occurrence time
- Call duration

Avaya J100 Series IP Phones store the call log in a file saved on the phone. J100 series phone software version 4.0.3 and later always encrypts the contents of the call log file.

If you downgrade the software of your phone to a version earlier than 4.0.3, you will lose the call log details.

Recents configuration

Use `46xxsettings.txt` file to set the following parameter:

Parameter name	Default value	Description
SOFTKEY_CONFIGURATION	0,1, and 2	Specifies which feature shows on which soft key on the Avaya J129 IP Phone screen. The options are: • 0 = Redial • 1 = Contacts • 2 = Emergency • 3 = Recents • 4 = Voicemail **Note:** Open SIP environment does not support emergency calls.
ENABLE_CALL_LOG	1	Determines whether call logging and associated menus are available on the phone. **Note:** Set this parameter to 0 to keep the user's data private before the user can access the phone.

Ringtones

By default, all Avaya J100 Series IP Phones have eighteen ringtones. You can add additional ringtones by setting the parameter RINGTONES in the `46xxsettings.txt` file.

In an open SIP environment, you can define whether the user can personalize the ringtone and manage the user experience with the phone.

Ringtone parameters

List of feature-specific `46xxsettings.txt` file parameters required to set the default ringtones:

Parameter	Default value	Description
RINGTONE_DEFAULT_ALTERNATE_NUM1	16	Specifies the index of the default ringtone to be used when an incoming call is from the first alternate number. Supported only in BroadSoft server. The operation values range between 1 to 18.
RINGTONE_DEFAULT_ALTERNATE_NUM2	17	Specifies the index of the default ringtone to be used when an incoming call is from the second alternate number. Supported only in BroadSoft server The operation values range between 1 to 18.
RINGTONE_DEFAULT_BLF_CALL_PARK	1	Specifies the index of the default ringtone to be used when a notification is received of a parked call on a BLF. The operation values range between 1 to 18.
RINGTONE_DEFAULT_BLF_INCOMING_CALL	1	Specifies the index of the default ringtone to be used when a notification is received of an incoming call on a BLF. The operation values range between 1 to 18.
RINGTONE_DEFAULT_CALL_FWD_RING	1	Specifies the index of the default ringtone to be used when an incoming call has been forwarded from another phone. The operation values range between 1 to 18.
RINGTONE_DEFAULT_CALL_PARK	1	Specifies the index of the default ringtone to be used when a notification that a call has been parked on the logged in extension. The operation values range between 1 to 18.

Table continues…

Parameter	Default value	Description
RINGTONE_DEFAULT_PRIMARY	1	Specifies the index of the default ringtone to be used when an incoming call is received which is not associated with any other ringtone based on the call type or a contact association. The operation values range between 1 to 18.
RINGTONE_DEFAULT_PRIORITY_ALERT	15	Specifies the index of the default ringtone to be used when an incoming priority call is received. Supported only in BroadSoft environment. The operation values range between 1 to 18.
RINGTONE_ALERTINFO	Null	Allows you to assign a specific ring tone to a call queue. Format: QueueID:SelectedRingtoneID[,QueueID:SelectedRingtoneID] Where QueueID is a free form string matching the call queue name, as configured in the server. SelectedRingtoneID is numerical index of one of the ringtones known to the phone. The operation value of the SelectedRingtoneID is between 1 to 18.
RINGTONE_DEFAULT_RING_REMINDER	18	Specifies the index of the default ringtone to be used when an incoming call is identified as a ring reminder. The operation values range between 1 to 18.

Ringtone parameters for all Open SIP environments

List of feature-specific `46xxsettings.txt` file parameters where you can define whether the users can personalize the ringtone:

Icon	Name	Description
PROVIDE_ALTERNATE_NUM1_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed
PROVIDE_ALTERNATE_NUM2_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed
PROVIDE_BLF_CALL_PARK_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed
PROVIDE_BLF_INCOMING_CALL_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed

Table continues…

Icon	Name	Description
PROVIDE_CALL_PARK_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed
PROVIDE_PRIMARY_RINGTONE_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed
PROVIDE_PRIORITY_ALERT_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed
PROVIDE_RING_REMINDER_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed

Feature configuration

Active call shortcut keys

With the Active call shortcut keys feature, the users can use Busy Lamp Field, Autodial, and Contacts keys as shortcuts to perform a specific action during an active call or, in some cases, during an active or a held call.

Using Autodial keys as shortcuts is available only in the Broadworks environment.

The following actions call can be specified for these keys:

- Attended call transfer: the phone puts an active call on hold, and the user can talk to the destination (a BLF user, an Autodial user, or a contact) first.
- Blind call transfer: an active call is immediately transferred to the destination.
- Conference call: the user can add another user to an active call to set up a conference.
- Call Park: the user can put an active call on hold or use a previously held call to resume it at the destination, that is, park this call at the destination.

Note:

Call park shortkey action is supported only in the Broadworks environment.

The Active call shortcut keys feature can be configured in either of the following ways:

- by setting the corresponding parameters in the `46xxsettings.txt` file
- by assigning shortcut actions to the required keys in the web interface

Related links

Settings field descriptions on page 157

Active call shortcut keys configuration

Use the `46xxsettings.txt` file to set the following parameters for Active call shortcut keys:

Parameter name	Default value	Description
SHORTCUT_ACTION_BLF	0	Specify the action performed if the user presses a BLF key, an Autodial key, or selects a contact on the Phone screen during an active or, in case of Call Park, an active or a held call. If a in Avaya Cloud Office™ environment a monitored BLF user has a DND presense status, the monitoring BLF user is not able to perform any action by pressing a BLF key.
SHORTCUT_ACTION_CONTACT		

Table continues…

Parameter name	Default value	Description
SHORTCUT_ACTION_AUTODIAL		Valid values: • 0: the active call is put on hold, and the destination extension number is dialed. • 1: the active call is put on hold, and the user can transfer this call immediately (blind transfer) or after talking to the destination first (attended transfer). If ENABLE_BLIND_TRANSFER is set to 1, the user can select between these transfer types. If ENABLE_BLIND_TRANSFER is set to 0, the user can make only an attended transfer. • 2: the active call is immediately transferred to the destination. If this value is used, it overrides the ENABLE_BLIND_TRANSFER parameter value. • 3: the active call is put on hold, and the call is established with the destination to set up a conference. • 4: the active or the held call is parked to the destination by appending the Park FAC with the destination extension number. **Note:** This value (“4”) is supported only in the Broadworks environment.

Adjusting the Sidetone level

Sidetone is the ambient noise that the users can hear as feedback when speaking on a handset or a headset.

To adjust the level of this feedback noise, you can set a required value to the following parameters in the `46xxsettings.txt` file:

Parameter name	Default value	Description
AUDIOSTHS	0	Specifies the level of sidetone in the handset. The options are: • 0: Normal level for most users. • 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.

Table continues…

Parameter name	Default value	Description
AUDIOSTHD	0	Specifies the level of sidetone in the headset. The options are: • 0: Normal level for most users. • 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. **Note:** Avaya J129 IP Phone does not support this parameter.

Anywhere and Mobility

With the Broadworks Anywhere feature, the user can make and receive calls from any phone using his work phone extension. The agent can use his personal mobile phone, a landline phone, a softphone or other device.

This feature can be useful if the agent wants to answer important calls when he is away from the office.

Broadworks Mobility allows to use a mobile device to access Broadworks features. This feature is a part of the Broadworks Anywhere solution.

The Broadworks Anywhere and Mobility features enable the user to perform the following tasks:

- make calls from any phone using the work phone extension
- move calls from the desk phone to any available phone
- move calls from the mobile phone to the desk phone (the Call Retrieve functionality)
- control availability by activating and deactivating the feature from the mobile device

Broadworks Anywhere and Mobility can be accessed and configured on the Broadworks web portal and in the Features menu of the phone.

Call Retrieve limitations

The following are the limitations for the Call Retrieve functionality:

- To retrieve an incoming call during an active call, the user must first hold the active call and then press **Call Retrieve**.
- Disable Broadworks Call Control Services for Call Retrieve to function properly. You can disable this feature on the Broadworks web portal or in the phone menu by toggling **BroadWorks Call Control** to off.

  For more details, refer to the Broadworks configuration guide or to the Features section of the phone user guide.

Avaya Spaces Calendar integration

Avaya Spaces is a cloud-based team collaboration and meeting application. The application offers instant messaging, voice and video communication, track communications, and manage tasks. For more information about Avaya Spaces, see *Using Avaya Spaces* guide.

With the Avaya Spaces Calendar integration feature, the user can press the Call soft key on the calendar appointment of the phone to join a meeting hosted on Avaya Spaces. The phone dials into the meeting phone number and enters the Space ID and password automatically.

The Avaya Spaces Calendar integration feature is optimized to work when meeting organizers use the Avaya Spaces Outlook plug-in. For more information about the Outlook plug-in, see the Microsoft Outlook Add-on section of the Avaya Spaces user guide.

You can configure the feature using the `46xxsettings.txt` file or the phone web interface.

Ensure that the Avaya J100 Series IP Phones access the Avaya Spaces cloud service at https://spacesapis.avayacloud.com for the feature to work. Set this URL in the parameter Spaces API URL in the phone web interface.

If required, enable the parameter APPLICATION_HEADER_APPEARANCE_CONTEXT for the phone screen to display the Calendar appointment title when the user presses the Call soft key from the Calendar application.

Note that Avaya J129 IP Phone does not support this feature.

Avaya Spaces configuration parameters

Use the `46xxsettings.txt` file to configure the following parameters:

Parameter Name	Default value	Description
SPACES_ACCESS_MODE	1	Specifies the authentication mode that can be used by the phone when connecting to Avaya Spaces. The options are: • 0: Disabled, all Avaya Spaces features via APIs are disabled. • 1: Guest only, Avaya Spaces feature can be accessed by guest/anonymous authentication only. Connections to Avaya Spaces uses the embedded public certificates and any certificates defined in the TRUSTCERTS. It ignores ENABLE_PUBLIC_CA_CERTS.
SPACES_DIRECT_NUMBER_DEFAULT	Null	You can define a direct number to use when attempting a call to Avaya Spaces. If the user does not select an Avaya Spaces direct number, this defined direct number is used. The value is a dialable string. Length can be up to 32 characters. Can contain the following: 0 to 9 digits, minus (-), parenthesis ((), comma (,), pound (#), asterisk (*), plus (+).

Table continues…

Parameter Name	Default value	Description
SPACES_DIRECT_NUMBER_PROVIDE	1	Specifies if the end-user can select a direct number for a voice call to Avaya Spaces. The options are: • 0: Hide, the user cannot select a direct number for a voice call to Avaya Spaces. Any previously selected direct number by the end-user is cleared. If SPACES_DIRECT_NUMBER_DEFAULT is not defined or found to not exist as a valid Direct Number, the user sees an error and warning pop-up on the phone screen. The phone does not display the Call soft key for the Avaya Spaces feature. • 1: Show, the user can select a direct number for a voice call to Avaya Spaces. **Note:** WLAN_COUNTRY is used to determine the location of the phone. The phone displays phone numbers based on this location. If you set the parameter WLAN_COUNTRY to a country that does not exist in the list of numbers provided by Avaya Spaces, then the phone number of the US is shown.

Configuring Avaya Spaces Calendar integration by using the web interface

About this task

Use the web interface of the phone to configure the required parameters to enable Avaya Spaces feature.

Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Settings**.
3. In the Avaya Spaces area, configure the required parameters.
4. Click **Save** to save the setting.

Related links

Settings field descriptions on page 157

BroadWorks advance call control

The end-users can remotely control the calls of their IP phone from their desktop soft client by using the BroadWorks advance call control feature.

The following features are supported remotely from the soft client:

- Remote call initiation: User can initiate an outgoing call from the phone remotely. The phone auto-answers the call from the soft client and initiates the outgoing call. If the user initiates a second call from the phone by using a soft client then the phone puts the first call on hold and auto-answers the second call and initiates the second outgoing call.
- Remote call hold and resume: User can hold an active call on the phone remotely. Also can resume a held call on the phone remotely. When there are several held calls, the user can choose which call to resume by using the soft client.
- Remote call answer: User can answer an incoming call on the phone remotely by using the soft client. When the user accepts the incoming call on the soft client, the phone auto-answers the incoming call. During an active call if the user receives another call, the user can answer the second call remotely by using the soft client. The first call is put on hold while the user answers the second call.
- Remote call conference: User can remotely initiate a conference call on an already active call.
- Remote call transfer: User can remotely transfer an already active call.
- Remote call release: User can remotely terminate an already active call.

The BroadSoft advance call control feature is available to all the users connected to the BroadSoft server. The end user can use the same credentials to log in to the phone and the BroadSoft soft client.

To enable the phone to auto-answer the incoming call, ensure to enable the AUTO_ANSWER_DURING_CALL parameter, and disable the AUTO_ANSWER_MUTE_ENABLE parameter.

For more information on configuring the soft client, see https://supportcenter.broadsoft.com/

Limitations

For using the soft client for the remote call initiation, ensure that you do not activate the local Call Forward always and DND features.

BroadSoft XSI support

The BroadSoft Xtended Service Interface (XSI) provides a set of APIs that enables telephony applications to integrate with BroadSoft servers to perform telephony-related functions in a BroadSoft communication network. Avaya J100 Series IP Phones deployed in a BroadSoft communication environment support BroadSoft XSI.

Avaya J100 Series IP Phones use the XSI interface to support the following Broadworks features:

- Directory

- Simultaneous Ring Personal
- Call Park/Unpark
- Call Forward Always
- Call Forward Busy
- Call Forward No Answer
- Do Not Disturb
- Call Waiting
- Anywhere
- Mobility

Note:

If you configure BroadSoft XSI, the following local features will not be available for the users. The administrator must enable these features on the BroadSoft server.

- Do Not Disturb
- Call Forward

BroadSoft Xtended Service Interface (XSI) configuration

Use `46xxsettings.txt` file to set the following parameters:

Parameter name	Default Value	Description
XSI_URL	Null	Specifies the FQDN or the IP address, HTTP or HTTPS mode and the port of the XSP server. If the value is defined, phone will initiate XSI connection establishment to retrieve the feature list. Default value: Port 80 is used for HTTP and port 443 is used for HTTPS if the port is not defined. For example: http://xsp1.iop2.broadworks.net or http://199.19.193.26

Table continues…

Parameter name	Default Value	Description
XSI_CHANNEL_DURATION	60	Specifies the time duration in minutes for XSI event channel. The phone will ask 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. Valid values are 60 to 1440 minutes.
XSI_HEARTBEAT	15	Specifies the interval in seconds to send heartbeat messages over Comet HTTP connection to XSP server of BroadWorks. Valid values are 1 to 999 seconds. **Note:** XSI_HEARTBEAT should equal to Broadsoft eventTimeout/2. The EventTimeout duration can be viewed in BroadSoft web interface.
FORCE_XSI_USER_ID	Null	Specifies the BroadSoft user ID which the phone must use for XSI authentication. BroadSoft user Id is the SIP user Id excluding at (@) and domain. Valid values are 0 to 255 ASCII characters.
FORCE_XSI_WEB_PASSWORD	Null	Specifies the BroadSoft's web portal password which the phone must use for XSI web authentication. If the value is null, then SIP authentication method is used.

Busy Lamp Field

With the Busy Lamp Field (BLF) feature, you can monitor the call status of other phones connected to the same network.

Important:

BLF lines are not call appearance lines and cannot be used to make calls.

This feature is available in both Broadsoft and Asterisk environments. See the environment specific information in notes.

Depending on the configuration, you can use BLF lines for specific tasks, such as:

- Monitoring the activity status of the phone
- Receiving incoming calls for another user (Directed Call Pickup)
- Speed Dial of the BLF user in an idle state
- Viewing outgoing call status
- Barging in on an active call
- Unparking a call (available only in the Broadsoft environment)

You can also assign BLF users to pre-configured line keys.

Note:

In the Broadsoft environment, you can change BLF line mapping on the Phone screen but not edit the BLF list.

Related links

Pre-configuration of keys on page 221

BLF configuration

Depending on the environment, the system administrator can configure the BLF feature in either of the following ways:

- `46xxsettings.txt` file (available in the Broadworks and other Open SIP environments).

  For Broadworks, use the `46xxsettings.txt` file only if Broadsoft Xtended Service Interface (XSI) is disabled. When XSI is enabled, phone will retrieve the BLF configuration from the Broadworks server and ignore the BLF parameters in the `46xxsettings.txt` file.
- the web interface of the Administration menu on the phone (available in the Broadworks and other Open SIP environments).
- Broadworks web portal (available only in the Broadworks environment). For more details, see the Broadworks configuration guide.
- Broadsoft Xtended Service Interface (available only in the Broadworks environment).

Related links

Configuration of soft key parameter for Busy lamp field call appearance states on page 245

BLF Alerting

You can configure the way the phone alerts users about BLF incoming and BLF parked calls. The available alert options are: None, Audial, Visual and Both. You can allow users to choose their preferred alert option, if you use non-forced configuration values, or force-configure one of the options.

If you select a non-forced configuration option, it becomes a default variant, still allowing the user to select their own option. Setting a forced option overrides user selection.

You can configure this feature through Web user interface under **Settings** menu in **Alerting on calls** and **Incoming call indication**.

In the `46xxsettings.txt` file, you can configure the following parameters for this feature: BLF_INCOMING_CALL_INDICATION, BLF_PARKED_CALL_INDICATION, BLF_INCOMING_CALL_INDICATION_MODE, BLF_PARKED_CALL_INDICATION_MODE.

Note:

This feature is available in 3PCC environment for Avaya J159 IP Phone, Avaya J169/J179 IP Phone and Avaya J189 IP Phone.

Prioritizing an incoming call over a BLF call

About this task

You can configure the phone to select a higher priority for users' own incoming calls over BLF calls and parked BLF calls.

Note:

This feature is available for in 3PCC environment for Avaya J159 IP Phone, Avaya J169/J179 IP Phone and Avaya J189 IP Phone.

Procedure

To configure this feature, do one of the following:

- In the `46xxsettings.txt` file, set the PRIORITIZE_OWN_INCOMING_CALL to 1 to enable the feature and to 2 to disable it.
- In the web User Interface, in **Settings**, select **Enabled** or **Disabled** in **Prioritize own incoming call**.

Enabling this feature establishes the following call priority in which the phone displays calls:

- Own incoming calls (older calls first)
- Own parked calls (older calls first)
- BLF calls (older calls first)
- BLF parked calls

If you disable the feature, the phone displays calls in order of appearance.

BLF call pickup from a monitoring phone

This feature allows users to pick up incoming calls made to a monitored BLF line using the monitoring phone. When the feature is enabled and the BLF user is in alerting state, users can pick up a call from a monitoring phone using the **Pickup** soft key or a corresponding line key.

You can configure this feature through the `46xxsettings.txt` BLF_PICKUP_METHOD parameter file or through the Web Interface in BLF Pickup Method in the Settings tab.

Note:

This feature is available in Ring Central environment for Avaya J159 IP Phone, Avaya J169/ J179 IP Phone, and Avaya J189 IP Phone.

BLF parameters

Use the `46xxsettings.txt` file to set the following parameters:

Parameter	Default value	Description

BLF_LIST_URI	None	Specifies a unique name for the BLF list of users that you want to monitor on the phone.
		In the Broadworks environment, this is a mandatory parameter for the BLF feature.
		In the Asterisk environment, you can either set BLF_LIST_URI or, if this parameter is not set, the phone reads the BLF value in the PHONEKEY parameter and assigns BLF lines with individual subscriptions to specified phone extensions.
		The BLF resource list has the following format:
		• `sip:[list name]@[domain]` or
		• `<list name>`
		For example,
		`SET BLF_LIST_URI sip:mylist1@devices.avaya.com`
		`SET BLF_LIST_URI sales`
		Note:
		Depending on the environment, to set this parameter, you must create a BLF URL on the Broadworks web portal or configure Resource List Subscription in the `pjsip.conf` file on the Asterisk server. For more information, see Broadworks configuration guide and Asterisk Project documentation.

Table continues…

Parameter	Default value	Description
BLF_LIST_PREFERRED_START_LOCATION	0	Specifies where the phone places detected BLFs on the home screen. The phone detects BLFs from BLF List URI. It provides the starting location from which the detected BLFs are placed. Valid values are 0 thourhg 96. **Note:** This parameter is supported only in the Broadworks and Asterisk environment. Valid values: 0 –BLFs will be placed depending on Button Module detection. Starting location is 1 if no BM. Starting location is 25 if a button module detected on the phone. 1-96 – Specifies the precise line key number.
BLF_LIST_LINEKEY_LOCATION_FORCED	1	Specifies if BLF line key placement is forced or not. When forced, the user cannot move, delete or relabel BLF line keys. **Note:** This parameter is supported only in the Broadworks and Asterisk environment. Valid values: 0 – Non-forced 1 – Forced It is recommended to use forced value for this parameter.
BLF_PICKUP_METHOD	0	Specifies whether pickup BLF call is using Invite with FAC in Request URI or using Invite with Replaces header. Value operation: • 0: Pickup BLF call using Invite with FAC in Request URI • 1: Pickup BLF call using Invite with Replaces header **Note:** This parameter is available in • Avaya J139 IP Phone • Avaya J159 IP Phone • Avaya J169/J179 IP Phone
CALL_PICKUP_BARGEIN_FAC	*33	Specifies the feature access code of Directed Call Pickup with Barge-In.
CALL_PICKUP_FAC	*97	Specifies the feature access code of Directed Call Pickup to pick up a call for a BLF user.

Table continues…

Parameter	Default value	Description
CALL_PARK_FAC	*88	Specifies the feature access code to park a call to a monitored line.
CALL_UNPARK_FAC	Null	Specifies the feature access code to unpark a call for a BLF user. **Note:** This parameter is supported only in the Broadworks environment.
PRIORITIZE_INCOMING_CALLS_LIST	0	Specifies whether visual display of incoming alerts are to be sorted when there is more than one or if they should be displayed in the order they are received. Incoming alerts can include (in priority order from high to low): incoming calls, calls parked to the user's extension, incoming calls to a monitored BLF key, calls parked to a monitored BLF key. Value operation: • 0: Sort the list of incoming alerts in the order they are received • 1: Sort the list of incoming alerts by priority **Note:** This parameter is available in • Avaya J159 IP Phone • Avaya J169/J179 IP Phone
ALLOW_BLF_LIST_CHANGE	3	Specifies whether a user can add or delete the monitored phone extensions from the BLF resource list. **Note:** This parameter is supported only in the Broadworks environment. Valid values: 0 – The user cannot add or delete monitored phone extensions. 1 – The user can only delete monitored phone extensions. 2 – The user can only add monitored phone extensions. 3 – The user can add and delete monitored phone extensions.

Table continues…

Parameter	Default value	Description
BLF_INCOMING_CALL_INDICATION	3	Specifies the indication type for a BLF incoming call. Valid values: • 0 - None (no alerting for BLF incoming calls). • 1 - Audible (only audible alerting for BLF incoming calls). • 2 - Visual (only visual alerting for BLF incoming calls). • 3 - Default (the behavior isl based on BLF_INCOMING_CALL_INDICATION_MODE parameter value). • 4 - Both (both audible and visual alerting for BLF incoming calls). **Note:** This parameter is supported only in the 3PCC environment.
BLF_PARKED_CALL_INDICATION	1	Specifies the indication type for a BLF parked call. Valid values: • 0 - None (no alerting for BLF parked calls). • 1 - Default (the behavior based on BLF_PARKED_CALL_INDICATION_MODE parameter value). • 2 - Audible (only audible alerting for BLF parked call). • 3 - Visual (only visual alerting for BLF parked call). • 4 - Both (default - both audible and visual alerting for BLF parked call). **Note:** This parameter is supported only in the 3PCC environment.

Table continues…

Parameter	Default value	Description
BLF_INCOMING_CALL_INDICATION_MODE	3	Specifies the indication mode for a BLF incoming call. Valid values: • 0 - None (no alerting for BLF incoming call). • 1 - Audible (only audible alerting for BLF incoming call). • 2 - Visual (only visual alerting for BLF incoming call). • 3 - Both (both audible and visual alerting for BLF incoming call) • 4 - Force None (forced only audible alerting for BLF incoming call). • 5 - Force Audible (forced only audible alerting for BLF incoming call). • 6 - Force Visual (forced only visual alerting for BLF incoming call). • 7 - Force Both (forced both audible and visual alerting for BLF incoming call). **Note:** This parameter is supported only in the 3PCC environment.
BLF_PARKED_CALL_INDICATION_MODE	1	Specifies the indication move for a BLF parked call. Valid values: • 0 - None (no alerting for BLF parked call). • 1 - Audible (only audible alerting for BLF parked call). • 2 - Visual (only visual alerting for BLF parked call). • 3 - Both (both audible and visual alerting for BLF parked call) • 4 - Force None (forced only audible alerting for BLF parked call). • 5 - Force Audible (forced only audible alerting for BLF parked call). • 6 - Force Visual (forced only visual alerting for BLF parked call). • 7 - Force Both (forced both audible and visual alerting for BLF parked call). **Note:** This parameter is supported only in the 3PCC environment.

Table continues…

Parameter	Default value	Description
PRIORITIZE_OWN_INCOMING_CALL	0	Specifies whether Prioritize own incoming calls over BLF calls feature is enabled or not. Valid values are: • 0 - Feature is disabled. The phone displays all calls in the order they are received. • 1 - Feature is enabled. The phone displays user's own incoming calls and own parked calls before BLF calls and BLF parked calls.
IGNORE_BLF_LINE_KEY	0	Specifies if Softkey1 action will not be performed when user presses line key associated with the BLF line. This parameter is not applicable when user presses BLF key in a conference, transfer, page target or similar selection mode. Value operation: • 0: Soktkey1 action is performed • 1: Soktkey1 action is not performed **Note:** Avaya J129 IP Phone does not support this feature.
SHORT_FORM_USER_ID	Null	Specifies if the users system extension number is different than the users FORCE_SIP_USERNAME and the user is monitoring other users via BLF. When the monitoring user attempts to place a call to a monitored BLF key it will prevent the J100 from displaying an incoming call for the BLF monitored user.

Related links

PHONEKEY parameter values on page 552

BroadWorks Directory

The BroadWorks Directory feature is used to search and view personal, group, and enterprise contacts. The following are the types of directories:

- Enterprise directory: To search and view the Active Directory global address list of an enterprise.
- Group directory: To view work, extension, and mobile numbers of contacts. You can place a call to anyone in this directory.
- Group common directory: To view names and phone numbers of the common contacts listed in the Group common directory.
- Enterprise common directory: To view names and phone numbers of common contacts listed in the Enterprise common directory.
- Personal directory: To view names and phone numbers of the contacts in the personal directory of the user. You can add, delete, or edit the contacts in this directory.

Note:

Avaya J129 IP Phone does not support the BroadWorks Directory feature.

Directory parameters

Use `46xxsettings.txt` file to set the following parameters:

Parameter	Default value	Description
BW_ENABLE_DIR	1	Specifies if directory contacts are available for processing. Operation values: • 0: Directory contacts are not processed and directory sources are not displayed to the user. • 1: Directory contacts are processed and directory sources are displayed to the user.
BW_ENABLE_DIR_ENTERPRISE	1	Specifies if Enterprise directory contacts are available for processing. Operation values: • 0: Enterprise directory contacts are not processed. • 1: Enterprise directory contacts are processed.
BW_ENABLE_DIR_ENTERPRISE_COMMON	1	Specifies if Enterprise common directory contacts are available for processing. Operation values: • 0: Enterprise common directory contacts are not processed. • 1: Enterprise common directory contacts are processed.
BW_ENABLE_DIR_GROUP	1	Specifies if Group contacts are available for processing. Operation values: • 0: Group contacts are not processed. • 1: Group contacts are processed.

Table continues…

Parameter	Default value	Description
BW_ENABLE_DIR_GROUP_COMMON	1	Specifies if Group Common contacts are available for processing. Operation values: • 0: Group common contacts are not processed. • 1: Group common contacts are processed.
BW_ENABLE_DIR_PERSONAL	1	Specifies if Personal contacts are available for processing. Operation values: • 0: Personal contacts are not processed. • 1: Personal contacts are processed.
BW_DIR_ENTERPRISE_DESCRIPTION	“Enterprise”	Specifies the display name for Enterprise directory.
BW_DIR_ENTERPRISE_COMMON_DESCRIPTION	“Enterprise Common”	Specifies the display name for Enterprise Common directory.
BW_DIR_GROUP_DESCRIPTION	“Group”	Specifies the display name for Group directory.
BW_DIR_GROUP_COMMON_DESCRIPTION	“Group Common”	Specifies the display name for Group Common directory.
BW_DIR_PERSONAL_DESCRIPTION	“Personal”	Specifies the display name for Personal directory.
BW_DIR_CUSTOM_DESCRIPTION	“Custom”	Specifies the display name for Custom directory.
BW_DIR_ENTERPRISE_EXTENSION	"BWEntr"	Specifies the display name for Enterprise directory extension.
BW_DIR_ENTERPRISE_COMMON_EXTENSION	"BW EnCom"	Specifies the display name for Enterprise Common directory extension.
BW_DIR_GROUP_EXTENSION	"BW Group"	Specifies the display name for Group directory extension.
BW_DIR_GROUP_COMMON_EXTENSION	"BW GrCom"	Specifies the display name for Group Common directory extension.
BW_DIR_PERSONAL_EXTENSION	"BW Pers"	Specifies the display name for Personal directory extension.
BW_DIR_CUSTOM_EXTENSION	"BW Cust"	Specifies the display name for Custom directory extension.

BroadWorks Call center

The BroadWorks call center feature is available in the following IP Phone models:

- Avaya J159 IP Phone
- Avaya J169/J179 IP Phone
- Avaya J189 IP Phone

You can enable the call center feature by using one of the following methods depending on the availability of XSI connection:

- BroadWorks web portal: You can use the BroadWorks web portal to activate call center feature. With the XSI connection you can assign call center services to the agents.
- `46xxsettings.txt` file: When there is no XSI connection, you can enable the feature by setting the value of the parameter BS_CC_ENABLED to 1 in the settings file. The phone ignores this parameter if XSI_URL parameter has the required value.
- Web interface of the phone: When there is no XSI connection, you can enable the feature by setting value Yes to the BroadWorks Call Center Enabled field. The phone ignores this parameter if XSI_URL parameter has the required value.

Depending on the agent requirement and license, you can assign the agents to one of the following call centers:

- Basic call center: Supports a simple call distribution and queuing scenario for a small work group. Inbound calls are distributed based on the agent's line state.
- Standard call center: Supports a normal call center environment with flexible routing options. The agent's workflow in this call center includes the ACD states.

  Any agent with a Standard or Premium call center license can be assigned to a Standard call center.
- Premium call center: Supports the most advanced set of routing and call management options for a formal call center environment. It supports ACD states, disposition codes to associate with ACD calls, and outbound calling.

  You can assign only agents with a Premium call center license to a Premium call center. A user with a Premium call center user license can be assigned to any call center type and any number of call centers.

For more information, see https://supportcenter.broadsoft.com/

Call center agent and supervisor

Supervisor

Using the BroadWorks web portal you can configure the supervisors of a call center and assign them to a call center. A supervisor can be any user in a group or an enterprise. You can obtain the details of the configured supervisors using the XSI connection. If the phone does not have the XSI connection, you can use the `46xxsettings.txt` file or the web interface of the phone.

Agent

The call center agent is a user who either periodically receives ACD-related calls along with direct inbound calls or who handles a high volume of inbound ACD calls in addition to making outbound calls. Using the BroadWorks web portal you can configure the agents of a call center and assign them to the call center and the supervisors.

For more information, see https://supportcenter.broadsoft.com/

Related links

Configuring Settings on page 155

Customer originated trace

Agents can initiate a call trace on obscene, harassing, or threatening call by using the Customer originated trace feature. They can initiate the feature on an active call or an immediate last call.

You can enable the feature from the BroadWorks web interface. For more information, see https://supportcenter.broadsoft.com/

Escalation calls to supervisor

The agents can escalate a call to their supervisors using the Escalation feature. You must assign the agents to the call center and the supervisors. The agents can choose the supervisors from the list of assigned supervisors during escalation.

Note:

If the BroadWorks call center feature is disabled, the agent cannot involve a supervisor in the escalation call.

Emergency escalation

In case of an escalation while handling a call center call, the call center agents can escalate an active call immediately to their supervisors using the Emergency escalation feature. You have to assign the agents to the call center and to the supervisors. The agents can choose the supervisors from the list of assigned supervisors during escalation.

Note:

If the BroadWorks call center feature is disabled, the agent cannot involve a supervisor in the escalation call.

Call disposition codes

Call disposition codes are available to the agents of the premium call centers to address multiple scenarios related to the call center calls. For instance, the agent can capture the result of a call, the call disposition could be the following: Requires Follow-Up, Issue Resolved, or Contacted Sales Rep etc. You can configure the call disposition codes using the BroadWorks XSI. If the phone does not have the XSI connection then you can configure the disposition code using one of the following:

- Web interface of the phone

- `46xxsettings.txt file`

Note:

The phone refreshes every 30 minutes to load if there are any new disposition codes, or to load the values immediately you can restart the phone.

Related links

Configuring Settings on page 155

BroadWorks call center parameters

Use the `46xxsettings.txt` file to set the following parameters:

Parameter name	Default value	Description
BS_CC_ENABLED	0	Specifies whether the BroadWorks Call Center feature is enabled or disabled. Use this parameter only if XSI is disabled (XSI_URL is empty). Options are: • 0: Disables the parameter. • 1: Enables the parameter. **Note:** This parameter is available in: • Avaya J159 IP Phone • Avaya J169/J179 IP Phone • Avaya J189 IP Phone

Table continues…

Parameter name	Default value	Description
BS_CC_UNAVAIL_CODES	Null	Specifies codes that the agent can select for the Unavailable state. Use this parameter only if XSI is disabled (XSI_URL is empty). You can enter the comma separated list of the reason codes and their descriptions in the following format: code = description. For example: 1= coffee break, 2= Tea party, dnd= Do Not Disturb **Note:** This parameter is available in: • Avaya J159 IP Phone • Avaya J169/J179 IP Phone • Avaya J189 IP Phone
BS_CC_AUTOMATIC_STATE	0	Specifies whether the agent state changes on the phone automatically when the agent logs in and logs out of the phone. The agent state is Sign in during log in and Sign out during log out. Options are: • 0: The phone will not automatically change the agent state. • 1: The phone will automatically change the agent state. **Note:** This parameter is available in: • Avaya J159 IP Phone • Avaya J169/J179 IP Phone • Avaya J189 IP Phone

Table continues…

Parameter name	Default value	Description
BS_CC_DISP_CODES	Null	Specifies call dispositions codes that the call center agents can apply to a call center call. You can enter comma separated string values of disposition codes. Disposition code does not support special characters. For example: 1=Follow-up required, sales:2=New customer, helpdesk:3=Issue resolved; 4=Issue unresolved. Here, 1 is available for all call centers, 2 is specific for sales, and 3, and 4 are specific for helpdesk. Use this parameter only if XSI is disabled (XSI_URL is empty). **Note:** This parameter is available in: • Avaya J159 IP Phone • Avaya J169/J179 IP Phone • Avaya J189 IP Phone

Table continues…

Parameter name	Default value	Description
BS_CC_SUPERVISORS	Null	Specifies the list of supervisors to whom the call center agents can call. You can enter comma separated string values of supervisors. For example : 6551=Supervisor1, sales:6552=Supervisor2, helpdesk:6553=Supervisor3; 6554=Supervisor4 Here, 6551 is available for all call centers, 6552 is specific for sales and 6553 and 6554 are specific for helpdesk Use this parameter only if XSI is disabled (XSI_URL is empty). **Note:** This parameter is available in: • Avaya J159 IP Phone • Avaya J169/J179 IP Phone • Avaya J189 IP Phone
ESCALATE_FAC	Null	Specifies the Feature Access Code to invoke Escalation feature. **Note:** This parameter is available in: • Avaya J159 IP Phone • Avaya J169/J179 IP Phone • Avaya J189 IP Phone

Broadsoft Call recording indicator

The Broadworks server provides functionality for active call recording. When the call recording feature is configured on the server, the phone can automatically record active calls. When this feature is enabled, the phone notifies users of the call being recorded using the LED indicator. When an active call is being recorded, the LED indicator is solid green. If an active call is not being recorded, the LED is solid red

For more information about configuring Call Recording on the Broadworks web portal, refer to Feature Reference documentation at https://www.broadsoft.com/.

This feature is available on Avaya J139 IP Phone, Avaya J159 IP Phone, Avaya J169/J179 IP Phone, and Avaya J189 IP Phones.

Call Park

The Call Park feature is used to put an active call on hold at a parking extension and retrieve the same parked call from another phone in the organization.

The phone supports two types of call parking:

- Park call: A user can park a call to a specific extension. When a call is parked, the extension where the call is parked displays a visual and audio alert.
- Group Call Park: A defined Call Park group member can park a call to any group member's extension, which other group members can pick up.

To configure the Call Park feature using the Broadworks web portal, see the Broadworks configuration guide.

Call decline policy

With the Call decline policy feature, users can decline an incoming call to not answer it. You can set the Call decline policy for the extensions. Depending on the set policy, a call can be declined with an audio message or a busy tone. You can set the Call decline policy for the incoming calls using one of the following methods:

- `46xxsetting.txt` file
- Web interface of the phone

This feature is available on BroadSoft and Asterisk environments. When you enable the Call decline policy feature, the user can decline the incoming calls of the following active features:

- Shared call appearance
- BroadWorks Anywhere
- BroadWorks Mobility

For BroadSoft environment, you can enable the feature using the BroadWorks web portal. For more information about BroadWorks, see https://supportcenter.broadsoft.com/

Avaya J129 IP Phone does not support this feature.

Call forwarding on a generic SIP server

With the Call Forwarding feature, you can divert incoming calls to another number.

You can configure Call Forwarding on a generic SIP server in either of the following ways:

- Enable or disable the feature on the phone web interface

- Set the required parameters in the `46xxsettings.txt` file

Configuring Call forwarding using the phone web interface

About this task

Use this procedure to enable or disable the Call forwarding feature using the web interface of the phone.

Procedure

1. Log in to the web interface.
2. In the navigation pane, go to **Settings**.
3. Select **Feature access**.
4. In the **Call Forward** field, click one of the following:
   - **Allow**: To enable call forwarding.
   - **Do not allow**: To disable call forwarding.

Call Forwarding configuration

Use the `46xxsettings.txt` file to set the following parameters:

Parameter name	Default value	Description
CALLFWDADDR	—	Sets the address to which the calls are forwarded. Users can change or replace this administered value if CALLFWDSTAT is not 0. **Note:** This parameter is supported when failed over from Aura SM to a non-Aura survivable server, excluding BSM.
CALLFWDDELAY	—	Sets the number of ring cycles before the call is forwarded to the forward or coverage address. The default delay is one ring cycle.

Table continues…

Parameter name	Default value	Description
CALLFWDSTAT	0	Sets the call forwarding mode of the phone by setting the following values: • 0: Disables call forwarding. • 1: Permits unconditional call forwarding. • 2: Permits call forward on busy. • 4: Permits call forward/no answer. Example: If you set a value of 6, the phone enables call forwarding on a busy tone and on no answer. **Note:** This parameter is supported when failed over from Aura SM to a non-Aura survivable server (excluding BSM).
COVERAGEADDR	—	Sets the address to which calls are forwarded for the call coverage feature. Users can change or replace this administered value if CALLFWDSTAT is not 0. **Note:** This parameter is not supported in an Open SIP environment.

Call forwarding on Broadsoft

The Broadsoft server provides the following Call Forwarding types:

- Call Forward: Diverts all incoming calls to another number.
- Call Forward Busy: Diverts incoming calls to another number if you are on a call.
- Call Forward No Answer: Diverts incoming calls to another number when you do not answer the call within a stipulated time.

In the environment with the Broadsoft server, the Call Forwarding feature can be configured in either of the following ways:

- by using the Main Menu of the phone.
- through the Broadsoft web portal.

For more information about configuring Call Forwarding on the Broadworks web portal, refer to Feature Reference documentation at https://www.broadsoft.com/.

For more details on feature configuration using the phone menu, refer to *Avaya J100 IP Phone Feature Reference: Do Not Disturb and Call Forwarding*.

Call Waiting

The Call Waiting feature is to used to get a notification about another incoming call even when phone has an active call. If this feature is enabled, the caller is put on waiting instead of hearing a busy tone.

The phone displays incoming call screen, plays incoming call ringtone, and the beacon LED flashes.

To configure Call Waiting feature by using the Broadworks web portal, see the Broadworks configuration guide.

Centralized call logs

You can configure the Centralized Call Log feature for the phone. Using this feature, you enable users to propagate their call logs to the RingCentral server and synchronize them with other devices and soft clients.

You can enable the Centralized Call Log feature only in the Avaya Cloud Office™ environment. All Avaya J100 Series IP Phones, except Avaya J129 IP Phone, support this feature.

You can configure centralized call logs in the `46xxsettings.txt` file with the help of `SET` operators.

Centralized call log parameters

Use the `46xxsettings.txt` file to set the following parameters for centralized call logs:

Table 2:

Parameter name	Default value	Description
CALL_LOG_MODE	0	Specifies if the phone uses centralized call logs. Value Operation: • 0: Local, the phone uses local call logs. • 1: RingCentral, the phone switches to centralized call logs.
ACO_CALL_LOG_REFRESH_INTERVAL	180,000	Specifies the time period after which the phone updates centralized call logs automatically. The valid value range is from 60,000 to 86,400,000 miliseconds.

Centralized personal contacts

You can configure the Centralized Personal Contact feature for the phone. Using this feature, you enable users to propagate their personal contacts to the RingCentral server and synchronize them with other devices and soft clients.

You can enable the Centralized Personal Contact feature only in the Avaya Cloud Office™ environment. All Avaya J100 Series IP Phones, except Avaya J129 IP Phone, support this feature.

You can configure centralized personal contacts in the `46xxsettings.txt` file with the help of `SET` operators. The phone ignores centralized personal contacts if:

- ENABLE_CONTACTS is disabled.
- REST_URL is not defined.

When you enable the Centralized Personal Contact feature or modify its parameters, the user needs to relog in.

Centralized personal contact parameters

Use the `46xxsettings.txt` file to set the following parameters for centralized personal contacts:

Parameter name	Default value	Description
PERSONAL_CONTACTS_MODE	0	Specifies if the phone uses centralized personal contacts. Value Operation: • 0: Local, the phone uses local contacts. 1: Server, the phone uses centralized personal contacts.
CENTRALIZED_PERSONAL_CONTACTS_REFRESH_INTERVAL	60	Specifies the time period after which the phone updates centralized personal contacts automatically. The valid value range is from 20 to 1,440 minutes. The parameter is valid when REST is enabled and CENTRALIZED_PERSONAL_CONTACTS_MODE is set to RingCentral.

Digit mapping

You can configure digit maps for the phone. This configuration completely replaces the use of the DIALPLAN parameter and Enhanced Local Dialing (ELD) to provide both a dial plan and dialing rules at the same time.

Using this feature, you can enable the following:

- Matching rules which trigger a matching dial plan
- Substitution rules to provide the same functions as ELD, such as prefix insertion and removal, addition of area codes and country codes.

This feature also enables the phone to block certain numbers from being dialed by users.

You can configure digital maps through the `46xxsettings.txt` file with the help of SET and ADD operators, which allows to use several digit maps. There is no set limit to the quantity of rules in a single digit map string, but a character limit of 255 characters for each string in a parameter value applies. You can also configure this feature using the web interface, which is the preferred way of configuration.

A digit map is a group of one or several rules, separated by commas (,). You can use blank spaces in digit maps for better readability, the phone ignores them when reading a digit map.

If a user dials a sequence that matches two or more rules in a digit map, the phone uses the exactly or most closely matching rule for that sequence.

Note:

This feature is not available in CCMS.

Digit mapping syntax

You can use the following elements to configure digit maps:

Element sign	Element name	Element description	Rule example
Any combination of: 0-9 * # + - A-Z a-z, excluding: x	Literals	Matches digit sequences with exactly the same literals. Use literals to explicitly match a string.	To explicitly match the phone number 1-212-555-7722, create the following rule from literals: • 12125557722 • 1 212 555 7722 You can add spaces for readability. Example: `SET DIGIT_MAPPING "12125557722,12125557724"` to precisely match these phone numbers
x	x	A wildcard element. Can stand for any character.	To create a rule for any 11 digit number started with 8831, use the following rule: • 8831 xxx xxxx

Table continues…

Element sign	Element name	Element description	Rule example
.	.Matching Function	A matching function matches 0 or more of the previous element, such as x. You can use it to capture a string of entered numbers or characters of arbitrary length.	To create a rule to use Australian international dialing notation, use the following rule: • 0011 64 x.
[ ]	Set	You can enclose a set of characters to match them to a single digit or character. You can use a set to match specific digits that form part of a number. Alphanumeric and wildcard characters are allowed inside a set, such as [x], [x#], [@#]..	The following set: [125-8] matches the numbers 1,2,5,6,7 and 8
[^]	Exclusion Set	An exclusion set matches any single alphanumeric character that is not within the set.	To match any arbitrarily long sequence of digits that does not start with 6,7,8,9, use the following matching rule: • [^6-9]x.
!	! Call Bar	To bar users from calling numbers that match a rule, add an exclamation mark (!) in front of that rule in the digit map.	To bar all calls to numbers starting with 1900, regardless of length, use the following rule: • !1900x.

Table continues…

Element sign	Element name	Element description	Rule example
< elements : literals >	Element to Literal Transformation	Enables replacing of numerals and/or characters sequence matching elements with given literals. The expression is contained within a set of pointy brackets (< >) -and elements are separated from literals using a colon (:). Use this rule to remove digits from a dialed number, add digits to a dialed number, or transform a dialed number. You cannot use single quote ‘ ‘ for the literals in this context. You can use special character as they do not apply in this context either. Elements can be empty, in which case you can omit the colon (:). The literals part can be empty too, but the colon (:) must not be omitted in this case. Both elements and literals cannot be empty at the same time.	• <112:000> - Take 112 and replace it with 000. • <02:>xxxx xxxx - Take 02, replace it with nothing, then match the next 8 digits. • <02>xxxx xxxx or <:02>xxxx xxxx - Add 02 to the start of an 8-digit number

Related links

Digit mapping parameters on page 295

Digit mapping parameters

Use the `46xxsettings.txt` file to set the following parameters for the digit mapping feature:

Parameter name	Default value	Description
ENABLE_DIGIT_MAPPING	0	Specifies if the phone uses DIGIT_MAPPING parameter for dial plan configuration, if the parameter is disabled DIALPLAN and ELD parameters are used. Value operation: • 0: Disabled • 1: Enabled
DIGIT_MAPPING	Null	Specifies a digit map the phone uses to match digits to ensure a complete number is dialed, to transform dialed digits, and block numbers from being dialed. ',' is used for rules separation. Valid value is a string of alphanumeric rules. If a rule uses incorrect characters, the phone ignores it. The preferred way of configuring this parameter is through the web interface.

Related links

Digit mapping on page 292

Downloadable directory

In generic and Asterisk Open SIP environments, you can upload or update the global contacts using the `.xml` file. The phone searches for any contacts at the reboot. If a new contact is available, the phone encrypts the contact and stores it in the flash memory. The Directory group of the phone displays the latest contacts.

Users of the phone cannot modify the contacts in the directory.

Note:

Avaya J129 IP Phone does not support Downloadable directory.

Updating and uploading the directory contacts

About this task

You can update the global directory contacts using the .xml file. Use the following procedure to update and upload the contacts file.

Before you begin

Ensure that you have at least one contact to update and upload to the directory of the phone.

Procedure

1. Enter the contact details in the .xml file in the predefined syntax.
2. Save the file in .xml format.
3. Store this file in the file server.
4. Do one of the following:
   - Update the parameter DOWNLOADABLE_DIRECTORY in `46xxsettings.txt` with the name of the file from step 2.
   - Update the **Downloadable Directory File Name** field in the Settings using web interface, with the name of the file from step 2.
5. Reboot the phone.

Result

The phone displays the latest directory contacts.

Related links

Downloadable directory syntax on page 545
Settings field descriptions on page 157

Display name configuration

This feature allows the administrator to set up a custom user Caller ID, which the remote party phone displays for calls instead of an extension number.

You can configure this feature on the SIP Account tab of the Web interface or through the `MACADDR.txt` and `46xxsettings.txt` files DISPLAY_NAME parameter.

Users can customize a default label, associated with the DISPLAY_NAME parameter. To enable this, you must set a value other than null for the parameter.

The Caller ID does not depend on first name and last name order and is displayed as is.

Display name configuration parameter

Use this parameter to configure Display name.

Name	Default value	Description
DISPLAY_NAME	Null	Specifies if the parameter will be used as the display name for the remote party if the server supports a phone providing its own display name. Not applicable for AURA and IPO/IPO CCMS. Parameter values must not include the following symbols: ";<>/&.

Distinctive Ringing

With the Distinctive Ringing feature, you can assign a different call ringtone for group calls or calls received from outside of the group.

Distinctive Ringing feature has the following functions:

- Priority Alert Ringing: To assign a different ringtone as a priority notification for specific incoming calls.
- Alternate Number Ringing: To enable different ringtones for alternate numbers of a Contact which can be differentiated from the primary phone number.
- Ring Reminder: To get a short ringtone as a reminder on the phone when the features like Call Forwarding Always and Do Not Disturb are enabled.
- Silent Alerting: To disable the audio notification and to get a visual alerting of an incoming call.

The Distinctive Ringing feature can be configured only on BroadSoft web interface.

For more information about configuring Distinctive Ringing on BroadSoft web interface, refer to *Distinctive Ringing Feature Description* at https://www.broadsoft.com/.

Distinctive Alert Waiting Tone

The Distinctive Alert Waiting Tone feature enhances the call waiting service by providing a distinctive ringtone to the caller when the called party is busy. The called party is alerted with a call waiting tone.

Distinctive Alert Waiting Tone includes the following features:

- Priority Alert Call Waiting Tone
- Alternate Number Call Waiting Tone

The Distinctive Alert Waiting Tone feature can be configured only on the BroadSoft web interface.

For more information about configuring Distinctive Alert Waiting Tone on BroadSoft web interface, refer to *Distinctive Alert Waiting Tone Feature Description* at https://www.broadsoft.com/.

Dynamic Park and Page

With the Dynamic Park and Page feature, users can park calls and announce the parked calls to other users.

This feature uses the servers dynamic park feature where the system assigns a dynamic park slot for each parked call. In Avaya Cloud Office™ environment, the phone displays the dynamically assigned park slot number which the user can use to make the page announcement.

Once the call is parked, the user can select from a list of page group or page extension targets depending on the configuration described in the following section.

Dynamic park and page configuration

Use the `46xxsettings.txt` file to set the following parameters:

Avaya J129 IP Phone does not support these parameters.

Parameter name	Default value	Description
CALL_PARK_DYNAMIC_METHOD	0	Specifies the method the phone uses to park an active call to a dynamic parking slot assigned by the server. Value operation: • 0: Blind Transfer: the active call is blind transferred to the CALL_PARK_DYNAMIC_FAC (Default). • 1: DTMF: provide the CALL_PARK_DYNAMIC_FAC digits into the active call.
CALL_PARK_DYNAMIC_FAC	Null	Specifies the Feature Access Code that the phone uses to park an active call to a dynamic parking slot assigned by the server.
CALL_PAGE_EXTENSION_FAC	Null	Specifies the Page feature access code used to inform the server to perform a page to an extension.

Table continues…

Parameter name	Default value	Description
ENABLE_PARK_DYNAMIC_AND_PAGE	0	Specifies whether the Park and Page feature is available to the user. The Park Dynamic and Page feature requires that the CALL_PARK_DYNAMIC_FAC code and CALL_PARK_DYNAMIC_METHOD are defined to park the call. Value operation: • 0: Park Dynamic and Page feature is not available to the user(Default). • 1: Park Dynamic and Page feature is available to the user.
CALL_PAGE_GROUP_FAC	Null	Specifies the Page feature access code used to inform the server to perform a page to a page group.

Table continues…

Parameter name	Default value	Description
CALL_PAGING_GROUPS	Null	Specifies a comma-separated list of paging groups a user can call (PagingGroupLabel:PagingGroup Address). "PagingGroupLabel" is a string describing the PagingGroupAddress. "PagingGroupAddress" is the address/number of the PagingGroupLabel. This parameter is used by ENABLE_PARK_DYNAMIC_AND _PAGE feature and displays the user a list of the PagingGroups when performing Park and Page. "PagingGroupLabel" up to 32 Unicode characters. "PagingGroupAddress" up to 64 alphanumeric chars, an extension, an address, or SIP URI. PagingGroupLabel and PagingGroupAddress can not contain: ;",=|<>/&, To add multiple paging groups, use **ADD** command. If you use several **SET** commands, the latest one overrides the previous one.

Force HTTP/HTTPS provisioning server credentials

You can pre-enter HTTP or HTTPS provisioning server credentials if your server requires authentication before the phone is deployed for usage. Forced configuration of server credentials is a safety measure to protect files on the provisioning server from unauthorized access, while still allowing the phone to access the server.

With the forced configuration of server credentials, end-users do not have to manually enter the username and password on their phones. Using a keyboard, administrators can create complex passwords for better security.

If the credentials are pre-configured, the user can work with the phone as if the server does not require authentication. If the credentials are not pre-configured or are changed, the user is prompted to enter their username and password to connect to the server.

You can configure HTTP/HTTPS provisioning server credentials through the web interface, DES, DHCP, and the `46xxsettings.txt` file parameters.

Web interface configuration

You can enter the username and password during the phone configuration process through the web interface. You can enter the HTTP provisioning credentials in the Management tab of the web interface.

DES provisioning

If you use DES for phone provisioning, you can obtain server credentials from the response URL. For example:

```
https://alice:myvoiceismypassword@provisioning.example.ca:8080/Avaya/
```

DHCP provisioning

If you use DHCP Option 242 to provision phones before the deployment, you can obtain provisioning credentials from the DHCP Option 242 server response.

Important:

If you configure provisioning server authentication through DHCP, the password string must not include the following symbols to avoid authentication and connection errors:

- Double quote mark (“ ”)
- Apostrophe (‘ ’)
- Comma (,)
- Equal (=)

PnP provisioning

If you use PnP to provision phones before the deployment, you can obtain provisioning credentials from the URL in the OOD Notify message. For example:

```
https://alice:myvoiceismypassword@provisioning.example.ca:8080/Avaya/
```

46xxsettings.txt file configuration

The server credentials are stored in the `46xxsettings.txt` file as FORCE_HTTP_AUTH_USERNAME and FORCE_HTTP_AUTH_PASSWORD parameter values. You can also configure these parameters through the `46xxsettings.txt` file directly.

Force HTTP/HTTPS server credentials parameters

You can configure the following parameters for HTTP/HTTPS provisioning server credentials.

Name	Default value	Description
FORCE_HTTP_AUTH_USERNAME	Null	Specifies the username for HTTP/HTTPS provisioning server authentication. The valid value is a string of up to 255 ASCII characters without any intervening spaces. Double quotes (“”) must not be used in a username string when you configure this parameter through the `46xxsettings.txt` file. The following symbols are not supported when provisioning the credentials with the DHCP Option 242: • Double quote mark (“”) • Apostrophe (’) • Comma (,) • Equal sign (=)
FORCE_HTTP_AUTH_PASSWORD	Null	Specifies the password for HTTP/HTTPS provisioning server authentication. The valid value is a string of up to 255 ASCII characters without any intervening spaces. Double quotes (“”) must not be used in password string when you configure this parameter through the `46xxsettings.txt` file. The following symbols are not supported when provisioning the credentials with the DHCP Option 242: • Double quote mark (“”) • Apostrophe (’) • Comma (,) • Equal sign (=)

Flexible Seating

With the Flexible Seating feature, the user can log in to another user's phone and access the settings configured for their primary phone.

The phone which is used for guest login is called a host device. The host phone must be provisioned with the host profile settings on the BroadSoft Device Management (BDM). The BDM switches the configuration files of the Flexible Seating host to those provisioned for the Flexible Seating guest service.

The primary phone and the host phone in Guest mode have the same set of configured features and can work simultaneously.

When a guest user logs in, the host device downloads the `MACAddr.txt` file and applies the guest phone settings. To download the configuration file, the host device must be connected to the BDM.

On the BDM, the Identity Device Profile of the host and guest phones must contain `%BWMACADDRESS%.txt` (the `MACAddr.txt` file) with the following content:

```
SET FORCE_SIP_USERNAME %BWLINEPORT-1%
SET FORCE_SIP_EXTENSION %BWAUTHUSER-1%
SET FORCE_SIP_PASSWORD %BWAUTHPASSWORD-1%
SET ENABLE_SIP_USER_ID 1
# Must be 1 if If BWLINEPORT-1 != BWAUTHUSER-1
SET BW_HOTELING_MODE %BWHOTELINGMODE-1%
# Block other login operations
SET PROVIDE_LOGOUT 0
SET GUESTLOGINSTAT 0
```

The administrator can add the required number of Flexible Seating host devices in the BroadSoft web interface. You might need the MAC address of the host device or the host user's credentials depending on the type of authentication used in the host device configuration.

During the first boot-up of the phone, you must specify the BDM IP address as a provisioning server address. If the phone has a different provisioning server address configured, you can change this setting in the Administration menu or the web interface.

When configured, the Flexible Seating feature is available in the Features menu of the host phone. Depending on the guest user status, the feature label can change from **Guest login** to **Guest logout**. When the feature is activated, the phone displays the Guest login screen with the **Username** and **Password** fields to enter the guest user's credentials. The top bar icons on the host phone indicates whether the guest user has logged in or logged out.

For more information about configuring Flexible Seating in the BroadSoft web interface, refer to *Flexible Seating Service Feature Description* at https://www.broadsoft.com/.

Flexible Seating limitations

The following are the limitations for the Flexible Seating feature:

- If the user unparks or retrieves calls using Call Unpark or Call Retrieve features on the host phone in Guest mode, these calls are not answered automatically but are displayed as incoming calls.

- The guest user must turn off the primary phone before using Flexible Seating on the host device and must log out from the host phone before using the primary device. Otherwise, the features configured on the BroadSoft XSI will not function properly.

Related links

IP configuration field description on page 95

Management settings field descriptions on page 187

Group Paging

Group Paging is a group feature that allows unidirectional paging for a group of users by dialing a group paging directory number or an extension. The feature can be configured by a group administrator or higher on BroadSoft web interface and by setting the required parameter in `46xxsettings.txt` file.

On BroadSoft web portal, Group Paging can be configured by the administrator in either of the following ways:

- setting up a special user account
- creating a paging group

For more information about configuring Group Paging on BroadSoft web interface, refer to *Group Paging Feature Description* at https://www.broadsoft.com/.

Group Paging configuration

Use the `46xxsettings.txt` file to set the following parameter for Group Paging:

Parameter name	Default value	Description
AUTO_ANSWER_MUTE_ENABLE	0	Controls the speakerphone muting when call is auto answered by phone.

Long-term acoustic protection

You can enable the long-term acoustic protection feature to protect the ears of the headset user. Long-term acoustic protection is supported only in L100 Series Headsets with RJ9 connector, when the headset profile is set to Profile1. You can configure this feature by using either the web interface or the `46xxsettings.txt` file.

Note:

Avaya J129 IP Phone does not support long-term acoustic protection.

Related links

Settings field descriptions on page 157

Long-term acoustic exposure protection parameter

Use the `46xxsettings.txt` file to set the following parameter.

Parameter name	Default value	Description
ACOUSTIC_EXPOSURE_PROTECT_MODE_DEFAULT	1	Specifies the acoustic exposure protection mode. The options are: • 1: Off • 2: Dynamic • 3: 4 hours • 4: 8 hours **Note:** Avaya J129 IP Phone does not support long-term acoustic exposure protection.

LDAP Directory

The LDAP Directory feature allows users to search contacts in any open source LDAP directory. When this feature is enabled, LDAP search appears in Contacts application on the phone. You can set up the parameters for an LDAP directory server using the web interface and the `46xxsettings.txt` file.

When searching for a contact, users can specify attributes in a search query and view up to 49 attributes for each match. The set of attributes depends on the selected LDAP server.

Users can select an LDAP server as a contact search source in **Applications** > **Contacts** > **Search** > **Sources**. When enabled, LDAP becomes the only available contact database, other contact databases are disabled.

Users can search any public LDAP directory that supports anonymous and authenticated requests through startTLS or ldaps:// protocol.

The user can successfully connect to the selected LDAP server using ldaps:// protocol if the following settings are configured:

- DIRSECURE=2
- DIRSRVRPRT corresponds to LDAPS port of the server
- DIRSRVR is FQDN
- server self-signed CA certificate is included in the TRUSTCERTS list

The LDAP Directory feature is not available in CCMS mode.

This feature is available on Avaya J139 IP Phone, Avaya J159 IP Phone, Avaya J169/J179 IP Phone, and Avaya J189 IP Phones.

Configuration of Binding to an LDAP server

When a user selects an LDAP server as a contact search source, the server authentication occurs through a bind operation. Binding allows users to access LDAP servers based on their client privileges.

LDAPv3 (RFC 2251) supports three types of authentication requests:

- Anonymous
- Simple Authentication
- Simple Authentication and Security layer (SASL)

When a client sends a request without a bind, and the DIRUSERNAME parameter has a null value, the LDAP server treats the request as anonymous. Some global servers support only authenticated requests using a username and a password.

The DIRAUTHTYPE parameter defines the binding type. There are several configuration scenarios:

- Simple binding
- SASL authentication

Simple binding

In this binding type, the DIRAUTHTYPE parameter is set to 0. DIRUSERNAME is DN of a record and DIRPASSWORD is the userPassword attribute of a record. The selected LDAP server is configured for read-only access for any user. In this case, when a user presses the **Search** soft key, the phone attempts a simple binding operation and displays the search results if the operation is successful.

SASL authentication

In this binding type, the DIRAUTHTYPE parameter is set to 1. The selected LDAP server is configured for SASL authentification and has DIGEST-MD5 and PLAIN in the supportedSaslMechanisms configuration attribute. If DIRUSERNAME and DIRPASSWORD parameter values are correct, when a user presses the **Search** soft key, the phone successfully binds to the LDAP server and sends a search request. If DIRUSERNAME and DIRPASSWORD are incorrect, the phone displays the following error message: `LDAP search unsuccessful due to server error. return code =23108.`

DIRAUTHTYPE is set to 1. DIRUSERNAME and DIRPASSWORD parameter values are correct. The LDAP server does not have DIGEST-MD5 but only PLAIN in the supportedSaslMechanisms configuration attribute. If TLS is enabled, when a user presses the **Search** soft key, and the phone attempts to bind to the LDAP server using the PLAIN mechanism. If this operation is successful, the phone sends a search request. If the binding fails, the phone displays an error message: `LDAP search unsuccessful due to server error. return code =23108.`

DIRAUTHTYPE is set to 1. DIRUSERNAME and DIRPASSWORD are correct. The LDAP server does not have DIGEST-MD5 but only PLAIN in the supportedSaslMechanisms configuration attribute. If TLS is enabled, when a user presses the **Search** soft key, the phone does not attempt to bind, but displays the following error message: `LDAP search unsuccessful due to server error. return code =23108.`

LDAP Directory configuration

Use the `46xxsettings.txt` file to set the following parameters for the LDAP directory:

Parameter name	Default value	Description
DIRENABLED_PLATFORM	0	Determines whether the LDAP directory search and application are enabled on the phone. Value operation: • 0: No • 1: Yes
DIRUSERNAME	Null	Specifies the LDAP client username. The following characters are allowed: • 0–9 • a-z • A-Z The preferred way of configuring this parameter is through the web interface.
DIRPASSWORD	Null	Specifies the LDAP client password. The following characters are allowed: • 0–9 • a-z • A-Z The preferred way of configuring this parameter is through the web interface.

Table continues…

Parameter name	Default value	Description

DIRSRVR	Null	Specifies the IP address or a fully qualified domain name (FQDN) of the LDAP directory server.
		The valid value is an IPv6 or IPv4 address in the dotted decimal format or a FQDN.
		For example,
		`SET DIRSRVR 192.168.161.54`
		or
		`SET DIRSRVR domain.com`

DIRSRVRPRT	389	Specifies the port number for the LDAP directory server. Valid values are positive integers from 1 to 65535. For example, `SET DIRSRVRPRT 389`
DIRTOPDN	Null	Specifies the LDAP search base. For example, `SET DIRTOPDN "dc=global,dc=avaya,dc=com"`

Table continues…

Parameter name	Default value	Description
DIRSECURE	1	Specifies whether to use TLS or TCP for the LDAP server. Value operation: • 0: Use TCP • 1: Establish TLS connection using the STARTTLS extended operation. • 2: Establish TLS connection using the Secure LDAP protocol (LDAPS) For example, `SET DIRSECURE 1` There is a difference between STARTTLS and LDAPS: STARTTLS uses the same port as the LDAP protocol. The DIRSRVRPRT parameter value must be the same as the port configured for the LDAP (not for LDAPS) protocol on the server side. The LDAPS protocol uses a port different from LDAP. The value for DIRSRVRPRT needs to correspond to server port for the LDAPS connection.

Table continues…

Parameter name	Default value	Description
DIRAUTHTYPE	1	Specifies the kind of authentication that is used if the value of the DIRUSERNAME parameter is not null. Value operation: • 0: Simple LDAP authentication. Normally the DIRUSERNAME parameter must contain a DN name of an LDAP record, and DIRUSERNAME must contain a password associated with the record. • 1: Simple LDAP Authentication and Security Layer (SASL). If a connection is established over TLS (DIRSECURE is set to 1 or 2), DIGEST-MD5 or PLAIN authentication mechanisms are supported. If the connection established over TCP (DIRSECURE is set to 0) DIGEST-MD5 is the only supported mechanism.
DIRSEARCH_FIELDS	"cn,sn,telephoneNumber"	Specifies LDAP search attributes. The exact number and names of the search attributes depend on the LDAP server configuration and can vary from one LDAP directory to another. When configuring the DIRSEARCH_FIELDS parameter, you must use attribute names that coincide with the selected LDAP server attribute names. For example, `SET DIRSEARCH_FIELDS "givenName,mail,middle initials, telephoneNumber,sn,mobile , o ,department ,Rank ,office ,DoD SIP URI"`

Table continues…

Parameter name	Default value	Description
DIRSHOW_FIELDS	"cn,sn,telephoneNumber,Mail"	Specifies LDAP detail show fields. The phone returns the attributes, specified in this parameter, for each match found for a search query. You can use this parameter to map the specified LDAP keywords. This mapping defines the way the phone displays the fields with LDAP details. For example, `SET DIRSHOW_FIELDS "dn=Distinguished Name,rank,gn=First Name,office=Office,middle initials=Middle Initial,Display Name=Full Name,sn=Last Name,job title=Job,cn=Common Name,o=Office,c=Country,department=Department,street=Street,mail=Mail Box,l,telephoneNumber=Phone Number,st,mobile=Mobile,postalCode=Postal code,facsimileTelephoneNumber=Fax,DoD SIP URI=Number"` In this example, the format is as follows: `SET DIRSHOW_FIELDS "[LDAP Attributes]=[Field Names],[LDAP Attribute 1]=[Field Name1]"`

Table continues…

Parameter name	Default value	Description
DIRNAME_FIELDS	cn	Specifies the attributes and their order, shown in the search results. Users can view other attributes, pressing the **Details** soft key. The attributes specified in this parameter must be a subset of the attributes specified in DIRNAME_FIELDS. For example, `SET DIRNAME_FIELDS "cn,sn"` In this example, each match on the search result list displays the last name and first name.
DIRNUMBER_FIELDS	telephoneNumber	Specifies the LDAP fields that contain a number a user can call to. The first number listed becomes the primary number. For example, `SET DIRNUMBER_FIELDS "telephoneNumber,mobile,DoD SIP URI"`

Table continues…

Parameter name	Default value	Description
DIR_TO_LOCAL_MAPPING	"displayName:Name,telephoneNumber:Work,mobile:Mobile"	Specifies mapping of LDAP fields to local contact fields. If there is no rule for at least one contact number, the entire contact mapping is disabled. Local contact field names can be assigned from the following: • "firstname" • "nickname" • "URI" • "extension" • "email" • "department" • "zipCode" • "country" for number types: • "work" • "home" • "mobile" • "other"
DIR_LDAP_DESCRIPTION	“LDAP Directory”	Specifies a custom label to be used for the LDAP directory in the Contacts application. Valid value is a text string.

Off-hook alert

This feature allows users to receive alerts when a phone is off the hook and idle. When it is enabled, the phone dials a preconfigured extension in the following cases:

- A user takes the handset off the hook and does not dial any digits for a set period of time after that.
- A user takes the handset off the hook, dials an incomplete or invalid phone or extension number, and does not end the failed session after a set period of time.

When the phone dials the off-hook alert destination extension, a user then has a two-way talk path with the monitoring extension.

You can configure this feature using the `46xxsettings.txt` file.

Note:

Phone lock and Shared Control features must be disabled for off-hook alert to work.

Off-hook alert parameters

Parameter name	Default Value	Description
OFF_HOOK_ALERT_TIMER	10	Specifies the length of the alert timer in seconds Value operation: • 1-60: timer in seconds
OFF_HOOK_ALERT_EXTENSION	Null	Specifies if the off-hook alert feature is enabled and the off-hook alert extension. Value operation: • "": Disabled • An extension number: The phone dials this number in case of an off-hook alert event.

Multicast Paging

With the Multicast Paging feature, the user can transmit a one-way RTP voice message to a group of phones within the same network.

The Multicast Paging group is defined by setting specific multicast IP address and port. The list of groups can be configured for every phone in the network, and a priority level can be defined for each outgoing group. Outgoing and incoming multicast page groups are configured separately so that the list of senders and recipients can vary.

An incoming multicast page is played on the phone speaker. The Phone screen displays a message box with the notification of an incoming multicast page during the transmission.

A multicast page can be sent to the configured groups either from the Features menu or, if the corresponding key is added, from the Phone screen. The user can add, move or delete the Multicast Paging keys from the Phone screen customization menu. During an outgoing transmission, the phone does not display any incoming calls but shows a message box indicating there is an outgoing multicast page. The user can activate any available audio device to send a page. The transmission is handled in a way similar to the outgoing call procedure.

If there is an incoming multicast page transmission with a higher priority, all other transmissions, including lower-priority pages and incoming calls, are ignored. Active calls have the priority level 3 and are put on hold when a multicast page with a higher priority is transmitted.

The Multicast Paging can be configured in either of the following ways:

- by setting the relevant parameters in the `46xxsettings.txt` file
- by defining the group list in the web interface

Multicast Paging does not depend on the SIP server and can be configured independently. However, the network used for Multicast Paging configuration must support multicast transmission. This feature is supported in all the environments.

Related links

Configuring Multicast Paging on page 205
Multicast Paging configuration on page 316

Multicast Paging configuration

Use the `46xxsettings.txt` file to set the following parameters for the Multicast Paging (MP) feature:

Parameter name	Default value	Description
MP_ENABLED	0	Specifies if the Multicast Paging feature is enabled on the phone. This is the basic parameter for this feature. If this parameter is not set, other parameters listed below will be ignored. Valid values: • 0: Multicast Paging is disabled. • 1: Multicast Paging is enabled.

Table continues…

Parameter name	Default value	Description

MP_GROUPS_TO_LISTEN	Null	Defines the list of Multicast Paging groups that the phone listens to. A maximum of 10 paging groups can be listed.
		
		The paging groups should be separated with a comma (“,”), and should be listed in the following format:
		
		`IP:port:priority:label`
		
		where
		
		• `IP` is the multicast IP address of an MP group;
		
		• `Port` is the IP port of a Multicast Paging group, the valid value is an even integer ranging from 1024 to 65534;
		
		• `Priority` is the priority of a group. Allowed values are 1 through 16, with smaller values indicating a higher priority;
		
		• `Label` is a group label which is displayed in notification messages when the incoming page from this group is played.
		
		All the above-listed settings are required.
		
		For example,
		
		`SET MP_GROUPS_TO_LISTEN “239.0.0.0:1208:1:Security, 239.1.2.3:1210:4:Sales”`

Table continues…

Parameter name	Default value	Description

MP_GROUPS_TO_SEND	Null	Defines the list of Multicast Paging groups which the phone can send pages to. Priority is not set for these groups. A maximum of 10 paging groups can be listed.
		The paging groups should be separated with a comma (“,”), and should be listed in the following format:
		`IP:port:label`
		`IP`, `Port`, and `Label` denote the same as the corresponding MP_GROUPS_TO_LISTEN values. All these settings are required.
		For example,
		`SET MP_GROUPS_TO_SEND “239.0.0.0:1208:Sales,239.1.2.3:1210:Team”`

MP_CODEC	1	Specifies a codec which will be used to code and decode Multicast Paging transmissions. Valid values: • 1: G.729 codec is used. • 2: G.711u codec is used. • 3: G.711a codec is used.
MP_PACKET_SIZE	20	Specifies the size of an RTP packet in milliseconds. The valid values are 10 through 80. The value must be valid for the selected codec and therefore must not be changed unless necessary.

Prioritization of codecs

This feature allows the administrator to set priority of use for all codecs, supported by the phone.

You can configure this feature through the web user interface in **SIP settings** > **Codec Priority** and in the `46xxsettings.txt` file.

If you do not set a codec priority, the phone uses the default priority.

Prioritization of codecs configuration

You can configure the following parameter for the Prioritization of codecs feature.

Name	Default value	Description
CODEC_PRIORITY	OPUS,G722,G711U,G711A,G726 ,G729	Specifies the priority order for all codecs, supported by the phones. Valid value is a string of correct codec names, separated by a comma with no blank spaces. For example: `SET CODEC_PRIORITY OPUS,G722,G711U,G711A,G726, G729` If values are entered incorrectly or the phone does not support the listed codec, the value is ignored.

Push

The Push feature allows trusted applications to send their content to Avaya J100 Series IP Phones without any action required from the user.

The Push process is a two-step operation which consists of the following:

- The Push request to the phone. The Push Initiator (PI), usually a server application, transmits a Push request via an HTTP POST method to the phone's Push Agent (PA).
- The Pull request to the trusted server. The Push Agent requests a URI of Push content from a trusted Push server.

The Push content is usually a WML file used by the WML browser or an XML file for setting up an RTP audio stream, displaying a message on the Top line, etc.

The requested Push capability can be one of the following types:

- `audio`: the phone receives or transmits a non-call-associated unicast RTP audio stream. The receive or transmit type is specified in the Push Content message.
- `display`: the phone downloads and renders a WML file in the browser.
- `receive`: the phone receives a non-call-associated unicast RTP audio stream.
- `subscribe`: the phone sends a Subscribe message to the server.
- `top line`: the phone downloads an `.xml` file that contains the text to display on the Top line.
- `transmit`: the phone transmits a non-call-associated unicast RTP audio stream.
- `multicast`: the phone receives a non-call-associated multicast RTP audio stream.
- `phonexml`: the phone downloads a `.phonexml` file.

The Push requests have two priorities, normal and barge-in, which corresponds to the two modes of a Push type: Normal and Barge.

Push configuration

Use the `46xxsettings.txt` file to set the following parameters for the Push feature:

Parameter name	Default value	Description
PUSHCAP	00000	Specifies the modes of each Push type that the phone supports. The Push value is a 3, 4 or 5 digit number, of which each digit controls a Push type and can be the following: • 0: All Push requests are rejected for this Push type. • 1: Only the Push requests with Barge mode are accepted for this Push type. • 2: The Push requests with Barge or Normal mode are accepted for this Push type. The following shows the Push types controlled by a PUSHCAP value of `21202`: • 2: Controls phonexml Push requests • 1: Controls transmit audio Push requests • 2: Controls receive audio Push requests • 0: Controls display Push requests • 2: Controls top-line Push requests **Note:** The display Push request (the WML browser) is not supported by the Avaya J129 IP Phone and the Avaya J139 IP Phone.
PUSHPORT	80	Specifies the TCP port number to be used by the HTTP server for Push. The allowed value is a positive integer from 80 to 65535.
TPSLIST	Null	Specifies a list of URI authority components from which Push content can be obtained. The list allows HTTPS with HTTP. Allowed values can contain up to 255 characters and must be separated by commas without any intervening spaces. **Note:** If TPSLIST is set to default, the Push feature is disabled.

Table continues…

Parameter name	Default value	Description
SUBSCRIBELIST	Null	Specifies a list of URIs to which the phone will send a subscribe message after the phone successfully registers with a call server, or when a subscribe push request is received with a type attribute all. The message is an HTTP GET for the URI with the phone's MAC address, extension number, IP address and model number appended as query values. The list can contain up to 255 characters. Values are separated by commas without any intervening spaces. If the value is set to null, subscribe messages are not sent.
PUSH_MODE	2	Specifies the combination of secure and non-secure Push to be used. The Push mode ranges from 0-2 and is of the following types: • 0: Only non-secure Push is enabled. • 1: Only Secure Push is enabled. • 2: Both secure and non-secure Push is enabled. **Note:** If PUSH_MODE= 2 (Both) subscribe using secure Push is attempted first, and if it fails, subscribe over non-secure is attempted.
PUSHPORT_SECURE	8443	Specifies the port for listening to the secure Push request. The secure push uses HTTPS.

Push-To-Talk

With the Push-To-Talk feature, a user can call another user and have the call answered automatically. This feature can be configured as a one-way or a two-way media connection.

The Push-To-Talk feature can also be configured when Automatic Answer is enabled.

The feature can be configured on BroadSoft web interface and by setting the required parameter in `46xxsettings.txt` file.

For more information about configuring Push-To-Talk on BroadSoft web interface, refer to *Push-To-Talk Feature Description* at https://www.broadsoft.com/.

Push-To-Talk configuration

Use the `46xxsettings.txt` file to set the following parameter for having a Push-To-Talk incoming call automatically answered:

Note:

Disabling this setting will affect other features like Call Unpark.

Parameter name	Default value	Description
AUTO_ANSWER_MUTE_ENABLE	1	Controls the speakerphone muting when call is auto answered by the phone. Value operation: • 0: Speakerphone is unmuted when the call is auto answered. • 1(Default): Speakerphone is muted when the call is auto answered.

Phone screen width

The phone screen width can be either forced or configured as a default layout which can the user can change later in the Settings menu of the phone.

The phone screen width is set in either of the following ways:

- by configuring the PHONE_SCREEN_MODE parameter in the `46xxsettings.txt` file
- by enabling the required mode in the web interface

Related links

Settings field descriptions on page 157

Phone screen width configuration

Configure the following parameter in the `46xxsettings.txt` file for setting the default screen width on the phone.

Important:

If the user has selected Half Screen mode in the Settings menu, changing PHONE_SCREEN_MODE from 0 to 1 will have no effect.

Parameter name	Default value	Description
PHONE_SCREEN_MODE	1	Specifies the screen mode used on the phone by default and whether the user can change this setting in the Settings menu. Valid values: • 0: Non-forced Half Screen mode is used by default, and the Display menu is available on the phone. The user can change the screen width setting manually to override the PHONE_SCREEN_MODE parameter value. • 1: Non-forced Full Screen mode is set. This is a default value which is used at the first boot-up of the phone. The Display menu is available under the Settings menu, and the user can change the screen width setting manually to override the PHONE_SCREEN_MODE parameter value. If PHONE_SCREEN_MODE is set to 1 after the phone screen mode is set to Half, this setting will have no effect. • 2: Forced Half Screen mode is used on the phone, and this setting cannot be changed by the user. • 3: Forced Full Screen mode is used on the phone, and this setting cannot be changed by the user.

Phone screen width limitations

The following are the limitations for changing the phone screen width:

- When you change the PHONE_SCREEN_MODE parameter value from Forced to Non-forced mode, the phone screen width will not switch automatically. However, the user can change it manually in the Settings menu of the phone.
- If you switch from Non-forced Half to Non-forced Full screen mode, the phone screen width will not change.
- When you switch from Non-forced Full to Non-forced Half screen mode, the phone screen width will change to half only if it is set to **Default** in the Settings menu.

Shared Lines

Shared Lines feature allows sharing of an extension across multiple phones to handle calls as a group. The feature has three modes:

- Shared Call appearance mode (SCA) available for Broadsoft environment
- Bridged Lines appearance mode (BLA) available for RingCentral and ACO environments
- Bridged Call Appearance mode (BCA) available for RingCentral and ACO environments

All phones sharing this extension support:

- Displaying incoming calls.
- Initiating outbound calls.
- Displaying the same caller ID for an outgoing call for all phones in the group.
- Displaying the state of all calls on the extension of all phones that share the extension.
- Joining calls on other phones in the group, if configured.
- Effective eliminating of any missed calls.
- Configuring call alerts and delayed ringing.

Note:

Avaya J129 IP Phone does not support Shared Lines.

Usage of SCA on the phone

Depending on the configuration, there are different approaches to how SCA can be used on the phone. The common configuration methods are Key System and Attendant Console.

Key System

A Key System configuration emulates legacy systems where many phones are configured with the same set of lines or extensions. For example, Key System might include four different extensions where the primary extension is configured as shared. All users with the same configuration will share the same extensions. Each configured extensions can be associated with a Direct Inward Dialing(DID) line and the incoming calls roll over to the next line when a line is busy.

Attendant Console

An Attendant Console configuration supports one phone to monitor the calls on multiple other phones. For example, the phone of an Executive Assistant can be configured with a shared extension of an Executive so that the Executive Assistant can answer incoming calls for the Executive or initiate outbound calls on behalf of the Executive. In this configuration, the Executive Assistant will have a primary extension that is private and one SCA for each Executive that the Executive Assistant supports. Each Executive will have only a primary extension which is shared.

SCA configuration

Extensions can be configured as Shared Call Appearance (SCA) on the Broadsoft server to be used as SCA or a primary shared extension on the phone.

Caution:

Assigning an extension to SCA on the phone when the extension is not configured as SCA on the Broadsoft server will result in unexpected behavior.

The following are three different ways to configure the phones to reflect the Broadsoft server SCA configuration.

- Using Broadsoft Device Management (BDM) to configure phones.
- Using the `46xxsettings.txt` file and MAC address files.
- Manually configuring SCA on the phone after logging in.
- Using web interface in **Shared Line Configuration**

With BDM, all SCA configuration in the Broadsoft server is automatically populated in the `46xxsettings.txt` file and MAC address file. Configuring the PROVIDE_SHARED_LINE_CONFIG setting to 1 prevents the user from altering the SCA configuration.

Manual configuration of SCA on the phone is available after a user has logged in and only if the PROVIDE_SHARED_LINE_CONFIG setting is equal to 2, which is the default. This method cannot be used to configure the primary extension as shared.

While BDM can be used to automatically create the appropriate `46xxsettings.txt` and `<MACaddress>.txt` files for each phone, it is also possible to manually configure these files. The capabilities of both methods are same, and all SCA settings are available.

Related links

Broadsoft Device Management on page 90
Shared Lines parameters on page 327

Bridged Lines Appearance mode

The BLA mode allows efficient distribution of incoming calls within a shared line group, eliminating the chances of missing an incoming call.

The same caller ID is displayed for the called party, when a call is initiated from any phone, belonging to a shared line group.

All phones within a shared line group can share and access a voicemail, receive alerts about calls on hold, contact other devices using paging and park calls from shared lines.

You can configure up to 10 shared lines in a single shared line group. Each line has its own call appearance.

Unlike in the Shared Call Appearance mode, users cannot modify the lines through **Menu** > **Settings**.

You can also configure your shared lines so that the phone displays only one shared call appearance for each shared line and supports either only Blind Transfer or Blind Transfer, Consult Transfer and Conference. This option is available in 3PCC only.

Depending on your server environments, you can select between the modes with the help of SHARED_LINE_MODE parameter in the `46xxsettings.txt` file.

The BLA mode is supported by RingCentral environment.

BLA configuration

BLA configuration is done through the`46xxsettings.txt` file and web interface under **Shared Line Configuration**. It is not recommended to manually change these settings. You can get the required settings for this feature using DES Provisioning server. RingCentral server automatically creates configuration files and adds MAC address of the phone to the RingCentral system.

The following settings are recommended for Ring Central Server:

- `SET SHARED_LINE_MODE 1`
- `SET SCA_LINE_SEIZE_DURATION 360`
- `SET OUTBOUND_SUBSCRIPTION_REQUEST_DURATION 360`
- `SET REGISTERWAIT 300`
- Configure the SOFTKEY_ACTIVE parameter for Call Park.

Bridged Call Appearance

Bridged Call Appearance or BCA mode allows efficient functioning or Boss/Assistant scenarios. This feature enables users of the same Shared Appearance Extension group to answer calls made to the same phone number from multiple devices.

The head of the group user can hand off answered calls to other users in the group. Assistant users can bridge to an active call, creating a conference.

With the Shared Lines feature, a primary user extension can be private or shared on the phone that owns a BCA group. A boss phone user can have up to 8 primary shared call appearances or up to 10 primary private call appearances. If a boss phone has private primary call appearances, it can also have up to 8 secondary shared call appearances.

Assistant phones of a BCA group always have at least one private line and up to 8 bridged call appearances for one boss phone. Assistant phones can be connected to up to 10 various boss phones. Call appearances on assistant phones with multiple bosses are grouped by boss. A boss user cannot bridge to other boss users.

This mode is available for Avaya Cloud Office™ environment.

Call alerts and delayed ringing configuration for shared lines

For each shared line, you can configure the type of incoming call indication, delayed ringing and beacon LED behavior. As an administrator, you can use forced configuration options or allow the user to choose a preferred option on their phones. You cannot configure these settings for a primary line, even if it is a shared line.

Alerting on calls configuration

You can configure the incoming call indication of the following types:

1. Visual, when the phone displays a pop-up message if there is an incoming call on a shared line
2. Audible, when the phone plays an audio signal if there is an incoming call on a shared line
3. Both audible and visual
4. None, in this case, the phone does not alert the user of an incoming call

5. Visual forced
6. Audible forced
7. Both forced
8. None forced

Delayed ringing configuration

You can also set up delayed indication for an incoming call on a shared line, if you do not want the phone to display an incoming call right away. You can use forced configuration options or allow the user to choose a preferred option on their phones.

Beacon LED configuration

You can configure the beacon LED behavior for an incoming call on a shared line. If you use an indication delay option, you can configure your beacon LED to start flashing immediately when the phone receives an incoming call or together with the ring. If your selected indication option is None or None forced, the beacon LED does not flash when there is an incoming call. This affects shared lines and BLF.

Shared Lines parameters

Use the `46xxsettings.txt` file to set the following parameters:

Parameter	Default value	Description
SHARED_LINE_MODE	0	Specifies whether the Bridged Line Appearance (BLA), Shared Call Appearance (SCA) or Bridged Call Appearance (BCA) mode is used. Value operation: • 0: Indicates Shared Call Appearance mode. • 1: Indicates Bridged Line Appearance mode. • 2: Indicates Bridged Call Appearance mode.
PRIMARY_LINE_TYPE	0	Specifies whether the phone's primary line is a private or shared line. If the primary line is a shared line, other settings that control the primary line behavior are not affected. Value operation: • 0: Indicates a private line. • 1: Indicates a shared line.
PRIMARY_LINE_EXTENSION	Null	Specifies the default label for primary shared and private lines. This value is used if the label for a primary call appearance is not customized. **Note:** This value is optional. If not provided FORCE_SIP_USERNAME value is used.

Table continues…

Parameter	Default value	Description
PRIMARY_LINE_BARGE_IN_ENABLED	1	Specifies whether the **Barge-in** soft key is displayed on the primary line if there is a call on this line on another device. Value operation: • 0: Indicates Barge-in is disabled for the primary line. • 1: Indicates Barge-in is enabled for the primary line. This parameter is ignored in BLA mode. **Note:** The RingCentral Server does not support **Barge-in** . This parameter value is ignored if the selected line mode is BLA.
SCA<n>_ENABLED	0	Specifies whether <n> shared line is enabled. <n> can be a number of 1 to 8. Value operation: • 0: Indicates disabled. • 1: Indicates enabled. Example: `SET SCA2_ENABLED 1` means the shared line 2 is enabled in any mode.
SCA<n>_MAX_CALL_APPEARANCES	1	Specifies the maximum number of simultaneous calls on each specified shared line. <n> can be a number of 1 to 10. This set of parameters provides independent control of the maximum number of call sessions on each shared line. This setting directly maps to the number of shared call appearances that are be displayed on the phone for this shared line. Values range from 1 to 8. **Note:** The RingCentral Server supports only 1 call appearance for each shared line. Even if the value is set otherwise, the server ignores it.
SCA<n>_SIPUSERID	Null	Specifies the Address or Record (AOR) for each shared line. This parameter is required for the SCA, BLA and BCA modes. <n> can be a number of 1 to 10. This parameter should only specify the handle, as the domain is specified independently. **Note:** Shared lines are only supported for the same SIP domain as the primary line.

Table continues…

Parameter	Default value	Description
SCA<n>_USERNAME	Null	Specifies the user name to be used for authentication when challenged with 401 for credentials on SIP requests associated with the shared line. <n> can be a number of 1 to 10. **Note:** This value is optional in SCA. If not provided, SCA<n>_SIPUSERID value will be used. In BLA mode, The RingCentral Server ignores this parameter and uses primary authentication credentials instead.
SCA<n>_PASSWORD	Null	Specifies the password used for authentication when challenged with 401 for credentials on SIP requests associated with the shared line. <n> can be a number of 1 to 10. This is a required parameter in SCA mode. **Note:** The RingCentral Server ignores this value and primary authentication credentials instead.
SCA<n>_EXTENSION	Null	Specifies the display name of the shared line. <n> can be a number of 1 to 10. The display name used for an idle shared line can be an arbitrary label and does not have to coincide with user's login credentials. **Note:** This value is optional. If not provided SCA<n>_SIPUSERID value is used.
SCA<n>_BARGE_IN_ENABLED	1	Specifies whether the Barge in option is enabled or disabled for each shared line on a BroadSoft server. When it is enabled, a user can barge into a call at a different location on the <n> shared line using a line key or a soft key. <n> can be a number of 1 to 10. Value operation: • 0: Barge in is disabled for the shared line. • 1: Barge in is enabled for the shared line. **Note:** The RingCentral Server does not support **Barge-in** . This parameter value is ignored if the selected line mode is BLA.

Table continues…

Parameter	Default value	Description
SCA_LINE_SEIZE_DURATION	15	In SCA mode, this parameter specifies the time in seconds that a shared line stays off hook with a dial tone when the call appearance is seized before the line transitions to a failed state. In BLA mode this parameter specifies the time in seconds for the inbound subscribe duration. Values range from 5 to 600. Recommended value for the RingCentral Server is 360.
PROVIDE_SHARED_LINE_CONFIG	1	Specifies if the user has the ability to change Shared Line configuration using the Settings menu on the phone. Value operation: • 0: Shared lines are not displayed in settings menu. • 1: Shared lines are displayed in settings menu but all information is read-only. • 2: Shared lines are displayed in settings menu and are fully configurable. This parameter value is ignored in BLA mode.
PRIMARY_LINE_EXTENSION	Null	Specifies the default label for primary shared and private lines. This value is used if the label for a primary call appearance is not customized. **Note:** This value is optional. If not provided FORCE_SIP_USERNAME value is used.
ANSWERED_ELSEWHERE_POLICY	1	Specifies if phones present missed call indication for calls, answered on other phones in the group. Value operation: • 0: The phone indicates calls answered on other phones of the shared line as missed. • 1: The phone logs calls answered on other phones of the shared line to answered calls.
SHOW_CALLFOR_ON_PRIMARY	0	Specifies whether incoming call pop-up messages are displayed with ‘Call for’ when a call is addressed to a primary private or shared line only. Value operation: • 0: The ‘Call for’ is not displayed. • 1: The ‘Call for’ is displayed.

Table continues…

Parameter	Default value	Description
SCA<n>_INCOMING_CALL_INDICATION_DEFAULT	3	Specifies the type of the incoming call indication on a shared line where <n> can be a number of 1-10. This parameter is applicable for SCA, BLA and BLF. If you use a forced value, the user is not able to change it. Value operation: • 0: None (no incoming call indication). • 1: Audible (the phone plays an audio signal) • 2: Visual (the phone displays a pop-up message) • 3: Both (audible and visual) • 4: None forced • 5: Audible forced • 6: Visual forced • 7: Both forced
SCA<n>_INCOMING_CALL_INDICATION_DELAYED_DEFAULT	0	Specifies the value in seconds, used by the phone to delay the displaying of call pop-pup and playing of ringtone for an incoming call. <n> can be a number of 1-10 Valid values are 0–99. If you use 0, there is no delay in alerting. This parameter is not used if you select None or None forced parameter values for SCA<n>_INCOMING_CALL_INDICATION_DEFAULT.
SHARED_CALL_APPEARANCES_MODE	0	Specifies the behavior of shared call appearances in BLA mode. The value for this parameter is valid only if SHARED_LINE_MODE is set to BLA. Value operation: • 0: The phone shows 1 shared call appearance and call appearance can perform only Blind Transfer. • 1: The phone screen shows 1 shared call appearance and the call appearance can perform Blind Transfer, Consult Transfer and Conference calls.

Table continues…

Parameter	Default value	Description
BEACON_INDICATION_MODE	0	Specifies the behavior of the beacon LED when the phone receives an incoming call. Value operation: • 0: The beacon LED starts flashing immediately when there is an incoming call until the call is answered or ignored. • 1: The beacon LED flashes after a delay as per delayed ringing configuration, when there is an incoming call and until call is answered or ignored This parameter applies to primary, shared, BLF and BLF parked lines.

Related links

SCA configuration on page 324
Broadsoft Device Management on page 90

Shared Lines limitations

The following limitations apply to the Shared Lines feature:

- The features that are assigned to a phone are associated with the primary phone extension and will only function on calls for the primary extension. For example, if a user enabled call forwarding, calls to the primary extension will be forwarded, but incoming calls to any configured Shared Call Appearance (SCA) will still be presented on the phone.
- Conference and Transfer can only be performed on a single extension. For example, a call on the primary extension cannot be joined into a conference with a call on SCA. Similarly, calls on two different SCAs cannot be joined together into a conference.
- Only Blind Transfer is supported in BLA mode because there is only one shared line appearance.
- Conferencing is not supported in BLA mode because there is only one shared line appearance.
- RingCentral server supports either private lines only or shared lines only, both are not supported simultaneously.

Note:

Set SHARED_CALL_APPEARANCES_MODE to 1, to support consult transfer and conference in BLA mode for single call appearance.

Scrolling mode

You can configure the phone to switch between line scrolling mode and page scrolling mode.

Line scrolling mode

Line scrolling mode is a single column mode where user scrolls the lists by lines using navigation keys.

Page scrolling mode

Page scrolling mode is a double column mode where use scrolls between pages with the help of **Left** and **RIght** navigation keys, and uses **Up** and **Down** navigation keys to navigate lines. When a selected line is in another page in this mode, it remains highlighted until the user manually deselects it.

You can configure this feature with the help of the `46xxsettings.txt` file or through the web interface.

Note:

This feature is available on Avaya J139 IP Phone, Avaya J159 IP Phone, Avaya J169/J179 IP Phones, and Avaya J189 IP Phone.

Scrolling mode parameter

You can configure the following parameter for the Scrolling mode feature.

Name	Default value	Description
SCROLLING_MODE	0	Specifies the scrolling mode used on the phone. Value operation: • `0`: Line scrolling mode is used. • `1`: Page scrolling mode is used.

Scrolling mode limitations

The following limitations apply to the Scrolling mode feature:

- **Calendar** days and details do not support Page Scroll mode.
- **Recents** view does not support Page Scroll mode.
- **Contacts** lists view and search results view does not support Page Scroll mode.

Shared Parking

The Shared Parking (SP) feature allows the user to park an active call to a shared phone extension which is also called a shared room. The Phone screen displays the SP extension as a BLF line. Other users with this feature configured on their phones can unpark the call from the shared room and resume the conversation.

The feature is available in NetSapiens environment on Avaya J159 IP Phone, Avaya J169/J179 IP Phones, and Avaya J189 IP Phone.

The Shared Parking icons reflect the state of the shared extension: idle or busy. The user can move the SP line to another location and customize its label. When the call is parked, the customized label changes to the caller's extension.

In addition to visual indication, when the call is parked, the phone plays an audio alert in the same way as for a BLF line in the parked state. You can customize the SP alert by selecting the required ringtone type in the Settings menu of the phone.

The call parking mode is determined by the SHORTCUT_ACTION_BLF_PARK parameter, and can be either of the following:

- by performing a blind transfer to the shared extension
- by dialing the Park FAC first and then dialing the shared extension number

You can add the Shared Parking key on the Phone screen as a pre-configured key either through the `46xxsettings.txt` file or in the web interface of the phone. On the web interface Key Configuration tab, the **BLF** and **BLFPark** type and name correspond to the Shared Parking feature.

Related links

Setting Pre-configuration of keys on page 207
PHONEKEY parameter values on page 552

Shared Parking configuration

Use the `46xxsettings.txt` file to set the following parameter for the Shared Parking (SP) feature:

Parameter name	Default value	Description
SHORTCUT_ACTION_BLF_PARK	0	Specifies the action which is performed when the Shared Parking line is activated during an ongoing call. Valid values: • 0: Blind transfer is performed to the SP extension number. • 1: The Park FAC and the SP extension number are dialed. This option might not be available in all the environments.

Selection of a higher priority line after ending a call

You can configure the phone to allow users to select a priority line after ending an active call.

When the feature is enabled, the selected Call Appearance (CA) remains prioritized after ending a call. The new call is received or initiated on the same CA. The prioritized line remains highlighted on the user phone screen. The user can manually switch to another line.

When the feature is disabled, after an active call ends, the CA is automatically switched to another line. The following priority order applies:

- The line with an active call.
- The line with the most recently held call or conference call.
- The line with the most recently held conference call.
- The first available line on the Phone screen.

You can configure this feature through the web interface or through the `46xxsettings.txt` file.

This feature is not supported in CCMS environment.

Note:

Avaya J129 IP Phone does not support this feature.

Selection of a priority line after ending a call parameter

You can configure the following parameters for this feature.

Name	Default value	Description
KEEP_CURRENT_CA	1	Specifies whether the currently active line on the phone screen is still highlighted after the call on the selected line is ended. Valid values: • 0 - Disable. When a call on the selected line is ended, the selection is moved from the current Call Appearance to session line with a higher priority or to the first available line if the phone becomes idle. • 1 - Enable (default). When a call on the selected line is ended, the highlighted line is not changed.

Server-initiated Update

With Server-initiated Update, you can get the notification from the SIP server if there are any available new settings or the phone firmware. If the file server has the requested files for update, the phone later applies new settings or, if available, updates the phone firmware.

By default, the Server-initiated Update feature is disabled. To enable this functionality, you must set the ENABLE_OOD_RESET_NOTIFY parameter to 1 in the `46xxsettings.txt` file.

When the phone receives a `SIP NOTIFY` message about available updates, it checks the `J100Supgrade.txt` file and compares the firmware version it contains to the current firmware

version. If the file server has a new firmware version, the phone reboots and upgrades to that version. If the firmware version stored on the file server and that of the phone match, the phone downloads the `46xxsettings.txt` file to apply the new settings. In this case, it either logs out the current user or, if required, reboots. If there are any active calls or other transmissions, the phone will apply the new settings only when it becomes idle.

The date and time of the last update are displayed in the Status tab of the web interface.

You can get the notification from the SIP server by using either of the following:

- the Administration menu of the phone
- the Management tab in the web interface

Related links

Updating phone settings and firmware on page 113
Status field description on page 121
Management settings field descriptions on page 187

Simultaneous Ring Personal

With the Simultaneous Ring Personal (SRP) feature, you can list up to 10 phone numbers or SIP-URI addresses you want to receive calls to in addition to the primary phone. This feature may be used when, for example, the agent is not at his desk phone and needs to answer a call from the cell phone. Simultaneous ring can be turned off when the agent is at the desk on a call.

Important:

If the cell phone has the voicemail which is activated before office voice messaging, the voice messages will be recorded in the cell phone database.

Simultaneous Ring Personal configuration

The administrator can configure the Simultaneous Ring Personal feature by using:

- Broadworks web portal.
- Phone menu.

For more information about configuring Simultaneous Ring Personal on Broadworks web portal, refer to Feature Reference documentation at https://www.broadsoft.com/.

For more details on feature configuration using the phone menu, refer to *Avaya J100 IP Phone Feature Reference: Simultaneous Ringing Personal*.

USB Headset

As an administrator, you can enable USB headset support. When this feature is enabled, a user can connect a USB headset to the phone like a plug-and-play device and switch between a wired headset, a bluetooth headset and a USB headset. When a USB headset is connected to the phone, an administrator can use the SNMP MIB browser to query for its details. You can also view USB headset details in the web user interface.

You can configure this feature using the `46xxsettings.txt` file or in the **Settings** tab of the web user interface.

This feature is available on Avaya J159 IP Phones and Avaya J189 IP Phones.

USB headset parameter

Use the `46xxsettings.txt` file to set the following parameter for USB headset:

Parameter name	Default Value	Description
ENABLE_USBHEADSET	1	Specifies whether the USB headset feature is enabled or not. Value operation: • 0: Disabled • 1: enabled

Note:

This parameter is applicable only if USBPOWER value is not 0 (a default value).

USB Flash drive

You can use the USB Flash drive support to copy the phone reports from phone to the USB device. The SNMP query is used for USB device information and configurable parameters. Configure this feature using the `46xxsettings.txt` file or in the **Settings** tab of the web user interface.

You can use the debugging parameters to view the issues in the USB log category.

The phone supports a flash drive with FAT32 file system.

This feature is available on Avaya J189 IP Phone and Avaya J159 IP Phones.

Connecting USB Flash drive

About this task

Use this procedure to connect the USB flash drive with phone.

Procedure

1. Plug in the flash drive to the USB port of the phone.

   The phone detects the flash drive, and `USB Flash Drive connected` text is displayed on the phone screen.

   If the phone does not identify the flash drive, `USB Flash Drive is not supported. Please try another one` text is displayed.

2. Press **Main Menu**.
3. Scroll to **Settings** and press **Select**.

4. Scroll to **USB** and press **Select**.

   You will view the flash drive in the list.

Generating phone reports

About this task

Use this procedure to generate phone reports or replace an existing phone report.

Before you begin

Ensure that USB flash drive successfully connects with the phone.

Procedure

1. Press **Main Menu**.
2. Scroll to **Administration** and press **Select**.
3. Scroll to **Debug** and press **Select**.
4. Scroll to **Phone report** and press on **Generate** soft key.

   The phone report is created, and `Storing phone report locally on the phone was successful` text appears on the phone screen.

   You can also replace an existing phone report.

Copying phone reports to USB flash drive

About this task

Use this procedure to copy the phone reports to the USB flash drive.

Before you begin

Ensure that the USB flash drive successfully connects with the phone.

Procedure

1. Press **Main Menu**.
2. Scroll to **Administration** and press **Select**.
3. Scroll to **Debug** and press **Select**.
4. Scroll to **Phone report** and press on **CopyToUSB** soft key.

   Once the phone report is successfully copied, `Copying phone report to a Flash Drive was successful` text is displayed on phone screen.

   Note:

   Do not unplug the USB flash drive while copying the phone report.

USB flash drive parameter

Use the `46xxsettings.txt` file to set the following parameter for USB flash drive.

Parameter name	Default Value	Description
ENABLE_USBSTICK	1	It enables or disables the USB flash drive support. This parameter ignores the other values if the value is set to 1 (enabled by default). Value operations: • 0: Disabled • 1: Enabled

Note:

This parameter is applicable only if USBPOWER value is not 0 (a default value).

USB keyboard

USB keyboard support is enabled by default. You can connect a USB keyboard to the phone and use the keyboard keys for entering texts and navigation. The SNMP query is used for USB keyboard information and configurable parameters. Configure this feature using the `46xxsettings.txt` file or in the **Settings** tab of the web user interface.

You can use the debugging parameters to view the issues in USB log category.

This feature is available on Avaya J189 IP Phone and Avaya J159 IP Phones.

USB keyboard parameter

Use the `46xxsettings.txt` file to set the following parameter for USB keyboard:

Parameter name	Default Value	Description
ENABLE_USBKEYBOARD	1	It enables or disables the USB keyboard support. This parameter ignores the other values if the value is set to 1 (enabled by default). Value operations: • 0: Disabled • 1: Enabled

Note:

This parameter is applicable only if USBPOWER value is not 0 (a default value).

WML browser

The WML browser feature allows the user to view WML web pages.

Wireless Markup Language (WML) is an XML-based markup language used by Avaya J100 Series IP Phones.

With the WML browser feature, the user can access a pre-configured Home page, **Click to Dial**, and **Add to Contacts** applications.

To create and edit a WML page, you can use off-the-shelf WML web authoring tools for intranet websites.

You can also enable users to pick up incoming calls from the WML browser application.

Note:

This feature is available only on the Avaya J159 IP Phone, Avaya J169/J179 IP Phone, and Avaya J189 IP Phone.

Related links

Nesting of WML elements on page 558
WML syntax specifications for Avaya J100 Series IP Phones on page 559

WML browser configuration

Use the `46xxsettings.txt` file to set the following parameters for the WML browser feature:

Parameter name	Default value	Description
WMLHOME	Null	Specifies the URL of a WML page to be displayed by default in the WML browser and if the **Home** soft key is selected. The allowed value contains not more than one URL of up to 255 characters. **Note:** If the value is set to default, the WML browser is disabled.

Table continues…

Parameter name	Default value	Description
WMLIDLEURI	Null	Specifies the URL for a WML page to be displayed when the telephone is idle for the time interval in minutes specified by the WMLIDLETIME parameter. The allowed value must contain not more than one URL of up to 255 characters.
WMLIDLETIME	10	Specifies the idle time in minutes, after which the web page set as the value of WMLIDLEURI is displayed. The allowed value is a positive integer from 1 to 999. **Note:** If WMLIDLEURI is set to null, the web page is not displayed when the phone is idle.
WMLPORT	8080	Specifies the TCP port number of the HTTP proxy server set as the WMLPROXY value. Allowed values are from 0 to 65535.
WMLPROXY	Null	Specifies the address of an HTTP proxy server that the WML browser uses. The allowed values must be in the dotted-decimal (IPv4) or DNS name format, separated by commas without any intervening spaces. The value can contain up to 255 characters.
WMLEXCEPT	Null	Specifies the IP addresses or domains for which the HTTP proxy server set as the WMLPROXY value is not used. Allowed values can contain up to 255 characters and must be separated by commas without any intervening spaces.

Table continues…

Parameter name	Default value	Description
ENABLE_WMLPUSH_ALERTING	0	Specifies the behavior of the WML browser during an incoming call. Value operation: • 0: The WML browser closes when the phone starts ringing and the phone displays an incoming call pop-up message. • 1: The WML browser remains open, and the user can pick up the incoming call by off-hook from a WBL browser application.

Voicemail

The voicemail feature is used to receive a voice message when user presses the **Message** button on the phone. Pressing the **Message** button asks for the voicemail number, which connects you to the voice mail system installed on the device.

You can use the PSTN_VM_NUM parameter in `46xxsettings.txt` file to configure the voicemail number.

Configuring voicemail by using the web interface

About this task

Use this procedure to configure the voicemail list in the web interface of the phone.

Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **SIP**.
3. In the Miscellaneous area, specify the number to access the voicemail in a non-Avaya environment.
4. Click **Save** to save the setting.

Voicemail configuration

Use the `46xxsettings.txt` file to set the following parameters:

Parameter name	Default value	Description
SOFTKEY_CONFIGURATION	0,1,2	Specifies which feature shows on which soft key on the Avaya J129 IP Phone screen. The features are defined as follows: • 0 = Redial • 1 = Contacts • 2 = Emergency • 3 = Recents • 4 = Voicemail **Note:** Emergency calls are not supported in an Open SIP environment.
PSTN_VM_NUM	Null	Specifies the dialable string that is used to call into the messaging system. For example, when you press the **Message Waiting** button. **Note:** This parameter is supported when the phone is failed over.

Visual voicemail

This feature allows users to handle voicemail. When this feature is enabled, users can playback voice messages, view their text transcript, mark them as read or unread, delete them and call back their sender. Voice transcripts depend on the server and are in the English language. They can also configure voicemail settings on their phone and view information and options for each message.

Administrators can configure a password to access visual voicemail on user phones.

This feature is configured with the help of the `46xxsettings.txt` file.

Visual voicemail is available for Avaya Cloud Office™ environment.

Visual voicemail parameters

Use the `46xxsettings.txt` file to set the following parameters:

Parameter	Default value	Description
PSTN_VM_NUM	PSTN_VM_NUM	Specifies the dialable string that is used to call into the messaging system. For example, when you press the **Message Waiting** button. If the value is Null, it brings up the Visual voicemail screen in Avaya Cloud Office™ environment. Value operation: • 0: Indicates Shared Call Appearance mode. • 1: Indicates Bridged Line Appearance mode. • 2: Indicates Bridged Call Appearance mode.
PSTN_VM_NUM	0	Specifies if the Visual voicemail feature is enabled. Value operation: • 0: Visual voicemail is disabled. • 1: Visual voicemail is enabled for Avaya Cloud Office™ environment.
VVM_PASSCODE_REQ	1	Specifies if a user needs a password to access Visual voicemail. If PHONE_LOCK_PIN is not defined, no password is required to access Visual voicemail. Value operation: • 0: Passwort is not required. • 1: Password is required.

Chapter 8: Security configurations

Security overview

SIP-based Avaya J100 Series IP Phones provide several updated security features. When the phone is in a locked state, the user can only receive calls or make emergency calls. User logs and data are protected with the user account.

Note:

The user cannot make emergency calls in an Open SIP environment.

The following security features are available:

- Supports X509v3–compliant certificates.
- Supports Identity certificate installation using the following methods:
  - Enrollment using Simple Certificate Enrollment Protocol (SCEP): Creates a private key and Certificate Signing Request (CSR) using the SCEP interface.
  - Importing key and certificate: Uses an encrypted PKCS#12 file format to import the private key and certificate.
- Supports Online Certificate Status Protocol (OCSP) for obtaining the revocation status of an X.509 Digital certificate.
- Supports Public Key Infrastructure (PKI) for users that use third-party certificates for all Avaya services including database.
- Supports VLAN separation mode using system parameter.
- Supports synchronization of system clock at configured intervals using system parameter.
- Supports display of SSH fingerprint in the ADMIN menu.
- Displays version of OpenSSH and OpenSSL in the ADMIN menu.
- Maintains the integrity and network protection under Denial of Service (DoS) attack, allowing the system to survive an attack without spontaneous rebooting and to recover to full mode automatically after the attack is over.

Important:

The ADMIN menu provides access to certain administrative procedures from the phone. You must change the default password for the ADMIN menu to restrict users from using the administrative procedures to change the phone configuration.

Locking and unlocking the phone

The user can lock the phone to prevent the use of the phone when they are away. Locking the phone does not log out the user, but the user can make emergency calls and receive calls. The user can lock the phone using the menu option in the phone.

You can set a PIN to unlock the phone. The user has to use the PIN you set to unlock the phone. You can set the limit on the number of failed attempts to unlock the phone. After the user exceeds the set limit you can block the user temporarily to unlock the phone. You can set the time period for which the users should be temporarily blocked.

You can use the one of the following to set the PIN, the limit on the failed attempts, and the time for blocking the user:

- `46xxsettings.txt` file
- Web interface of the phone

If you do not set a PIN, the SIP password is the default value for unlocking the phone. Even if you use the default password, you can set the limit on the number of failed attempts, and set a time period to temporarily block the user.

Phone lock configuration parameter

Configure the following parameters using the `46xxsettings.txt` file:

Parameter	Default value	Description
PHONE_LOCK_IDLETIME	0	Specifies the interval of idle time, in minutes, after which the phone will automatically lock. Value operation: • 0: Phone will not lock automatically. Valid values are 0 through 10,080.
PHONE_LOCK_PIN	Null	Specifies the PIN that you set for the user to enter it to unlock the phone. The value can be only digits, ranging between 4–20 characters. if you do not set any value here, the SIP password can be used for unlocking the phone.

Table continues…

Parameter	Default value	Description
PHONE_LOCK_PASSWORD_FAILED_ATTEMPTS	0	Specifies the number of consecutive failed attempts that you permit to unlock the phone. After the maximum is reached, the user will be blocked from further attempts for a period of time before being allowed to attempt again. If you set the value to 0, the user will never be blocked from attempting to unlock the phone.
PHONE_LOCK_PASSWORD_LOCKED_TIME	5	Specifies the length of time that you set where the user will be blocked from attempting to unlock the phone if the user exceeds the maximum number of failed unlock attempts. The value ranges between 5–1440 minutes.

Access control and security

Phones provide several security features for control and access. These include:

Security event logging

Logs are maintained for the following events:

- Successful and failed logins, username lockouts, and registration and authorization attempts by users and administrators.
- Change in roles.
- Firewall configuration changes.
- Modification or access to critical data, applications, and files.

Private Key storage

The phone stores the private key in PKCS#12 file format. The phone sends the device identity certificate and a private key along with the encrypted password to the WPA supplicants. MD5 passwords are sent to the WPA supplicants securely.

Temporary Data

The phone deletes any temporary storage data from the program, variables, cache, main memory, registers, and stack.

IP information

The phone enables the user with ADMIN privileges to see the IP information on the phone screen.

The parameter PROVIDE_NETWORKINFO_SCREEN controls the display information.

OpenSSH/OpenSSL version

The phone displays the version of OpenSSL and OpenSSH on the VIEW screen in the ADMIN menu. To see this information, set the parameter DISPLAY_SSL_VERSION to `1`.

SSH Fingerprint

The phone displays the SSH fingerprint to manually verify that an SSH connection is established with the correct phone.

Time synchronization

The phone synchronizes the time with the configured NTP servers in intervals. Use the parameter SNTP_SYNC_INTERVAL to check the time interval for synchronization. The range is 60 to 2880 minutes, and the default is 1440 minutes.

HSTS

The phone sends the HTTP Strict Transport Security (HSTS) header in the HTTP response. If the parameter ENABLE_HSTS is set to 1, the phone sends the header only when the web UI is accessed over the HTTPS.

The available values for the parameter:

- 0: Disabled (default)
- 1: Enabled

FIPS mode

The Federal Information Processing Standard, or FIPS 140-2, is a computer security standard for cryptographic modules used by the U.S. government. FIPS 140-2 specifies the security requirement that a cryptographic module must meet to protect the classified or sensitive data.

OpenSSL libraries include a set of cryptographic algorithms compliant with FIPS 140-2, which is invoked when the library is initiated in FIPS mode. You can enable the FIPS mode using the FIPS_ENABLED parameter that controls the usage of OpenSSL FIPS-certified cryptographic modules. You can set the parameter through the `46xxsettings.txt` file or DHCP option 242.

Note:

In FIPS mode, the CONFIG_SERVER_SECURE_MODE parameter value should be set to 1 ensuring only HTTPS is used to access the configuration server.

Disable the following features when enabling the FIPS mode on the phone:

- SSH Server.
- SCEP certificate enrollment: When a phone runs in FIPS mode, identity certificate enrollment through SCEP is disabled by the software. If identity certificate is generated before FIPS_ENABLED is set to 1, it can still use the existing identity certificate after phone reboot. However, you must not use identity certificates generated using SCEP when FIPS_ENABLED is set to 0 and the phone is configured to work in FIPS mode. The most secure way to install identity certificate is to clear any installed identity certificate and install

PKCS#12 file after configuring the phone to FIPS mode. Thereafter, FIPS 140-2 approved cryptographic algorithms can be used to decrypt PKCS#12 file.

- SLA Mon.
- 802.1x with EAP-MD5 or EAP-PEAP authentication. EAP-TLS is allowed.
- WML Browser.
- Push.
- HTTPSRVR. You must use TLSSRVR for file downloading.
- HTTP in OCSP_URI or Authority Information Access (AIA) of a certificate. Ensure that the URI in OCSP_URI or AIA of a certificate is HTTPS.
- Microsoft™ Exchange

Once you enable FIPS mode, the phone reboots and runs the OpenSSL FIPS self-test. After the test is completed successfully, the phone displays the message `FIPS mode activated, restarting...`. After reboot, FIPS mode is in effect. If the FIPS-mode self-test fails, the phone displays the message `FIPS self-test failure`. Here the phone also displays two options:

- **Program**: The phone prompts for a CRAFT password. After you enter the CRAFT password, the phone boots up in non-FIPS mode.
- **Reboot**: The phone reboots.

Note:

All the logs are stored in SYSLOG. These logs might be referred to for the troubleshooting purpose.

Related links

FIPS mode parameter on page 349

FIPS mode parameter

You can set the following parameter in the `46xxsettings.txt` file

Parameter name	Default Value	Description
FIPS_ENABLED	0	This parameter is used for enabling FIPS mode on the phone. Setting the value to 1 specifies only FIPS-approved cryptographic algorithms are supported. Value operation: • 0: No restriction on using non-FIPS approved cryptographic algorithms. • 1: Use only FIPS-approved cryptographic algorithms using embedded FIPS 140-2-validated cryptographic module.

Related links

FIPS mode on page 348

Geographical restrictions on encryption

Starting from R.4.0.4., SRTP is not supported on Avaya J100 Series IP Phones sold in Russia, Belarus, Kazakhstan, Kyrgyzstan, and Armenia to meet local restrictions on the use of encryption.

On such phones, the settings related to SRTP are excluded both from the phone interface and the web interface, and the administrator cannot enable SRTP.

Certificate management

Certificates are used to establish a secure communication between network entities. Server or mutual authentication is used to establish a secure connection between a client and a server. The client always validates the server certificate and maintains a trust store to support this validation. If the server additionally requires mutual authentication, it requests an identity certificate from the client. The client must provide the identity certificate, and the server must validate the certificate to establish mutual authentication. The server must validate the identity certificate to establish a secure connection.

Phones support three types of certificates:

- Trusted certificates
- Online Certificate Status Protocol (OCSP) trust certificates
- Phone identity certificates

The Trusted and OCSP trust certificates, are root or intermediate Certification Authority (CA) certificates that are installed on the phone through the `46xxsettings.txt` file.

You can use the following enhancements for installing identity certificates:

- SCEP over HTTPS is supported for enrollment.
- PKCS#12 file format is supported for installation.

If the log level is maintained, the users are notified through a log message WARNING with the category CERTMGMT. The logs are maintained and displayed if SYSLOG is enabled.

MIB object tables and IDs are created for certificates installed on the phone. You can view the certificate attributes through an SNMP MIB browser.

To implement DES, the phone has 64 Public CA certificates built-in. For a list of the certificates, see Public CA Certificates on page 574.

Related links

Public CA Certificates on page 574

Identity certificates

Identity certificates are used to establish the identity of a client or server during a TLS session. Phones support the installation of an identity certificate using one of the following methods:

- Secure Certificate Enrollment Protocol (SCEP) by using the `46xxsettings.txt` file parameter MYCERTURL.

  ```
  SET MYCERTURL "http://192.168.0.1/ejbca/publicweb/apply/scep/
  pkiclient.exe"
  ```

- PKCS12 File by using the `46xxsettings.txt` file parameter PKCS12URL.

  ```
  SET PKCS12URL http://192.168.0.1/client_$MACADDR_cert.p12
  ```

You can view the following attributes of the certificate using an SNMP MIB browser:

- **Serial Number**
- **Subject Name**
- **Issuer Name**
- **Validity Period**: **notBefore** and **notAfter** dates
- **Thumbprint**: Hash of the certificate
- **Basic Constraints**
- **Subject Alternative Name**
- **Key Usage Extensions**
- **Extended Key Usage**

To validate the identity of a received certificate, the following process is followed:

- Verification of certificate chain up to the trusted entity.
- Verification of the signature.
- Verification of the revocation status through OCSP.

- Verification of the certification validity (not-before and not-after dates are checked).
- Verification of the certificate usage restrictions.
- Verification of the identity against the certificate.

Subject Alternative Field (SAN)

While validating the certificates, the phone verifies whether the presented certificate has a SAN field or not. The SAN field simplifies the server configuration. With the SAN field, you can specify additional host names, such as IP addresses or common names, to use a single SSL Certificate.

- If the certificate does not have the SAN field, the phone validates the Common Name (CN) fields of the certificate. In this case, you need the following CN fields:
  - **SIP domain name**
  - **IP address**
- If the certificate has the SAN field, the following attributes for an HTTP-TLS connection are present:
  - Provisioning phone with only an IP address
    - In the **SAN** field, IP attribute with IP of HTTPS server is present.
  - Provisioning phone with FQDN of HTTPS server
    - In the **SAN** field, IP attribute with the IP address of HTTPS server is present.
    - DNS attribute with FQDN of HTTPS server.

Note:

While provisioning the phone with the FQDN of HTTPS server, you need two attributes in the **SAN** field:

- DNS attribute with FQDN
- IP attribute IP address

Trusted certificates

Trusted certificates are the root certificates that are used to verify the received certificates. These certificates are installed on the phone through the http server using settings file and are used to validate server certificates during a TLS session.

OCSP trust certificates

Online Certificate Status Protocol (OCSP) is used to check the certificate revocation status of an x509 certificate in use. The phone needs to trust the OCSP server and its CA certificates must be installed on the phone. These certificates are called OCSP Trust Certificates.

OCSP Trust Certificates are installed in the same way as those for System Manager. However, OCSP Trust Certificates use a different parameter name called OCSP_TRUSTCERTS. This parameter follows the same format as that for TRUSTCERTS.

Key Usage check for security certificates

This feature allows administrators to enable or disable Key Usage and Extended Key Usage checking in server security certificates.

You can configure this feature through the web interface or using the `46xxsettings.txt` file.

Related links

Key Usage checking configuration on page 353

Key Usage checking configuration

You can configure the following parameter for the Key Usage and Extended Key Usage checking in server security certificates:

Name	Default value	Description
KEYUSAGE_REQUIRED	0	Specifies whether the server certificate is checked for the presence of a Key Usage extension. When enabled, a server certificate is rejected if the Key Usage extension is missing. Value operation: • 0: Key Usage checking is disabled • 1: Key Usage checking is enabled

Related links

Key Usage check for security certificates on page 353

Parameter configuration for secure installation

For a secure installation, configure the following parameters:

Parameter	Set to	Notes
TRUSTCERTS		Provides the file names of certificates to be used for authentication. It supports both root and intermediate certificates and can contain up to six certificate files.

Table continues…

Parameter	Set to	Notes
AUTH	1	Ensures usage of HTTPS file servers for configuration and software files download. After AUTH is set to 1 and the device downloads the trusted certificates, the device can only download files from an HTTPS server. That server must have certificates that can be validated using a trusted certificate repository. You can change this parameter value back to 0 only by resetting the phone to defaults.
SSH_ALLOWED	0	Keeps SSH disabled.

SCEP parameters

Configure the following Simple Certificate Enrollment Protocol (SCEP) parameters:

Parameter	Type	Default value	Description
MYCERTURL	String	Null	Specifies the URL to access the Simple Certificate Enrollment Protocol (SCEP) server. The device attempts to contact the server only if this parameter is set to other than its default value.
MYCERTCN	String	$SERIALNO	Specifies the Common name (CN) for SUBJECT in the SCEP certificate request. The values can be $SERIALNO or $MACADDR. If the value includes the string $SERIALNO, that string will be replaced by the phone's serial number. If the value includes the string $MACADDR, that string will be replaced by the phone's MAC address.
MYCERTDN	String	Null	Specifies the common part of SUBJECT in SCEP certificate request. This value defines the part of SUBJECT in a certificate request including Organizational Unit, Organization, Location, State, and Country that is common for requests from different devices.
MYCERTKEYLEN	Numeric	2048	Specifies the private key length in bits to be created in the device for a certificate enrollment. The range is from 1024 to 2048.

Table continues…

Parameter	Type	Default value	Description
MYCERTRENEW	Numeric	90	Specifies the percentage used to calculate the renewal time interval out of the device certificate's Validity Object. If the renewal time interval has elapsed, the phone starts to periodically contact the SCEP server again to renew the certificate. The range is from 1 to 99. The phone starts using the new certificate immediately after the renewal, even when it is in use, for all new TLS connections. All existing connections are not broken.
MYCERTCAID	String	CAIdentifier	Specifies the Certificate Authority Identifier. Certificate Authority servers might require a specific CA Identifier string to accept GetCA requests. If the device works with such a Certificate Authority, the CA identifier string can be set through this parameter.
SCEPPASSWORD	String	$SERIALNO	Specifies a challenge password to use with SCEP. The value of SCEPPASSWORD, if non-null, is included in a challengePassword attribute in SCEP certificate signing requests. If the value contains $SERIALNO, $SERIALNO is replaced by the value of SERIALNO. If the value contains $MACADDR, $MACADDR is replaced by the value of MACADDR without the colon separators.
SCEPENCALG	0	Specifies SCEP Encryption Algorithm. Value operation: • 0: DES • 1: AES-256 **Note:** Avaya J129 IP Phone supports this parameter.	SCEPENCALG

Chapter 9: Data Privacy Controls Addendum

Purpose

Data privacy controls addendum applies to Avaya J100 Series IP Phones.

Personal Data is stored internally in the phone's flash file system which is not directly externally accessible except through SSH to the limited privilege "craft" user via an Avaya EASG login. Filesystem content is not encrypted except for passwords. When Personal Data is being transmitted over a network, it is encrypted with the most up-to-date protocols.

Related links

Configuring Data Privacy on the Avaya J179 IP Phone

Data categories containing personal data (PD)

User data (in memory)

Calls: Remote party phone number

Conference calls: participant display name, roster list

End user preferences information

Device configuration information

Contacts retrieved from network

User data (on flash)

Device configuration information

End user preferences information

Call Logs (on flash)

Local call logs

User Passwords (on flash)

User's SIP password, WiFi password, EAP password, http password, local Admin password

User data in logs (on flash)

User handle, SIP user name, display name information from SIP messages.

Personal data human access controls

User data (in memory)

- No Access

User data (on flash)

- SSH – Limited to Avaya Services login to the “craft” account with EASG authentication. “craft” account has limited access to filesystem.
- Web Admin – Access is limited to a predefined “admin” account where the password is defined by the customer. Access is provided to most configuration settings and some user settings.

Call Logs (on flash)

- No Access

User Passwords (on flash)

- No Access

User data in logs (on flash)

- SSH – Limited to Avaya Services login to the “craft” account with EASG authentication. “craft” account has limited access to filesystem.
- Web Admin – Access is limited to a predefined “admin” account where the password is defined by the customer. Access provides the ability to download a Phone Report which contains log files.

Related links

Personal data programmatic or API access controls on page 357

Personal data programmatic or API access controls

User data (in memory)

• Internal programmatic access.

User data (on flash)

• None

Call Logs (on flash)

•None

User Passwords (on flash)

•None

User data in logs (on flash)

•None

Related links

Personal data human access controls on page 357

Personal data at rest encryption controls

User data (in memory)

- Not encrypted by phone application except for passwords stored in memory. Passwords are only decrypted temporarily during use.

User data (on flash)

- Not Encrypted

Call Logs (on flash)

- Not Encrypted

User Passwords (on flash)

- AES-256 encrypted
- There are no controls available for the type or strength of encryption

User data in logs (on flash)

- Not Encrypted

Personal data in transit encryption controls

User data (in memory)

- TLS 1.2 to send/receive data with servers

User data (on flash)

- TLS 1.2 (HTTPs) to send/receive data with servers
- SSH

Call Logs (on flash)

- TLS 1.2 (HTTPs) to receive data with servers
- Data is never transmitted out of the phone

User Passwords (on flash)

- TLS 1.2 to send/receive data with servers (only the encrypted form is transmitted)

User data in logs (on flash)

- TLS 1.2 (HTTPs) to send data with servers when it is being sent as a phone report
- SSH

Personal data retention period controls

User data (in memory)

- In-memory data is removed based on use cases. For example, during a call, a call object remains in memory. When the call ends, the object is removed from memory, but a new CallLog object is created.

User data (on flash)

- Permanent until rolled over, or until the device is reset to defaults

Call Logs (on flash)

- Permanent until rolled over, manually deleted by the user, or until the device is reset to defaults

User Passwords (on flash)

- Permanent until rolled over, or until the device is reset to defaults

User data in logs (on flash)

- Permanent until rolled over, or until the device is reset to defaults

Personal data export controls and procedures

User data (in memory)

- Not applicable

User data (on flash)

- Using the phone Administration menu, an Administrator can generate a Phone Report containing configuration data which is transmitted if an external backup server is configured via the BRURI setting
- While logged in to craft via SSH, configuration data can be transmitted.
- While logged into an Admin Web page, configuration data can be viewed and exported or a Phone Report can be generated and saved.

Call Logs (on flash)

- No export capability is provided

User Passwords (on flash)

- No export capability is provided

User data in logs (on flash)

- Using the phone Administration menu, an Administrator can generate a Phone Report containing logs which is transmitted if an external backup server is configured via the BRURI setting
- While logged in to “craft” via SSH, log files containing user data can be transmitted
- While logged into an Admin Web page, log files containing user data can be exported

Personal data view, modify, delete controls and procedures

User data (in memory)

- Not applicable

User data (on flash)

- The User can modify and delete settings from the local menu on the phone
- The Administrator can modify and delete selected data using the Administration menu on the phone
- The Administrator can modify and delete selected data using the Admin web page

Call Logs (on flash)

- The User can delete individual log entries or all log entries from the local menu on the phone
- The Administrator can delete all call logs using the Reset to Defaults function in the Administration menu on the phone
- The Administrator can delete all call logs using the Reset to Defaults function in the Admin web page

User Passwords (on flash)

- The User cannot directly modify passwords
- The Administrator can delete all passwords using the Reset to Defaults function in the Administration menu on the phone
- The Administrator can delete all passwords using the Reset to Defaults function in the Admin web page

User data in logs (on flash)

- The User has no ability to modify or delete log files
- The Administrator can delete all log files in the phone using the Reset to Defaults function in the Administration menu on the phone
- The Administrator can modify and delete selected data using the Admin web page or delete all data using the Reset to Default function

Personal data pseudonymization operations statement

User data (in memory)

- Not applicable

User data (on flash)

- Not applicable

Call Logs (on flash)

- Not applicable

User Passwords (on flash)

- Not applicable

User data in logs (on flash)

- Not applicable

Data privacy and secure data processing

Avaya J100 Series IP Phones provide measures to ensure data privacy and secure processing of personal data. You can configure the phones in a secure mode to encrypt personal data at rest and end-to-end encrypt personal data in transit.

Secure mode

In secure mode, phones provide secure processing of personal data. Internal configuration files are encrypted and any internally generated logs and reports do not persist for longer than 24 hours. You can manually generate a new phone report in secure mode, but the phone deletes it 8 hours after its creation.

Secure mode activation

By default, Secure mode is off on the phones. You can activate secure mode by using one of the following methods:

- In the `46xxsettings.txt` file, set the ENABLE_GDPR_MODE parameter to `1`.
- In web interface, navigate to **Settings** > **Privacy** > **GDPR mode** and set it to `Enable`

Secure mode deactivation

You can deactivate Secure mode by using one of the following methods:

- In the `46xxsettings.txt` file, set the ENABLE_GDPR_MODE parameter to `0`.
- In web interface, navigate to **Settings** > **Privacy** > **GDPR mode** and set it to `Disable`

Related links

Configuring secure mode parameter on page 362
Configuring Secure Mode on the Avaya J179 IP Phone

Configuring secure mode parameter

You can configure the following parameter to enable secure mode.

Name	Default value	Description
ENABLE_GDPR_MODE	0	Specifies if data security and privacy mode is applied on the phone. When this parameter is enabled, the phone doesn't store any personal data without encryption for a period of more than 24 hours. Value operation: • 0: Secure mode is disabled (default) • 1: Secure mode is enabled

Related links

Secure mode on page 361

Data privacy

In addition to activating the secure mode, you must use the following configuration to ensure user data is private:

- Contacts: disable by setting the following `46xxsettings.txt` parameter:

  ```
  SET ENABLE_CONTACTS 0
  ```

- Recents: disable by setting the following `46xxsettings.txt` parameter:

  ```
  SET ENABLE_CALL_LOG 0
  ```

  Note:

  The phone deletes existing Recents logs when you apply this setting.

- Force HTTPS for configuration and disable Web Server: set the following `46xxsettings.txt` parameters:

  ```
  SET ENABLE_WEBSERVER 0
  ```

```
SET AUTH 1
```

- Logs: by default, logs are protected, because the SSH server is disabled by default. Logs are internal to the phone and, with GDPR mode activated, are cleared every 24 hours. To maintain these settings, do not set the SET SSH_ALLOWED parameter value to other than 0. To protect logs, use the following `46xxsettings.txt` parameters:

  ```
  SET SYSLOG_LEVEL 1
  SET SYSLOG_ENABLED 0
  SET LOGSRVR ""
  SET LOG_CATEGORY ""
  ```

You can also enable the Secure Syslog feature. If you choose this option, use the following configuration:

`SET SYSLOG_ENABLED 1`

`SET LOGSRVR "xx"` where xx is an FQDN address for a TLS server.

Enable the Phone Lock feature

To enable the Phone Lock feature, you need to provide SIP login and password information to the user.

You can configure the Phone Lock feature so that users can manually lock their phones using the **Lock** soft key on the Idle phone screen or the **Lock** feature key. You can also set the idle time interval after which the phone automatically locks.

To do this, set the following `46xxsettings.txt` parameters:

- `SET ENABLE_PHONE_LOCK 1`
- `SET PHONE_LOCK_IDLETIME`: use any value other than 0 for this parameter to set the idle time interval.

Additional settings

The following settings are turned off by default, but if you want to ensure that data privacy is maintained as required, make sure you observe the following settings:

- `SET SNMPADD ” “`
- `SET TPSLIST ” “`
- `SET SLMSTAT ” “`

Use HTTPS values for the following settings:

- `USER_STORE_URI`
- `XSI_URL`
- `CONFIG_SERVER_SECURE_MODE` — do not set to 0

Use TLS values for the following settings:

- `SIP_CONTROLLER_LIST`
- `SIP_CONTROLLER_LIST_2`

- `SET SIPSIGNAL 2` — TLS is used by default
- `SET ENABLE_OOD_MSG_TLS_ONLY 1` — TLS is used by default

Secure Syslog

The Secure Syslog feature enables you to select between a secure and non-secure modes for syslog messages transportation. When you select the secure syslog mode, the phone carries out all syslog events reporting over a secure TLS channel. When you select the non-secure mode, the phone uses a UDP channel.

When in the secure syslog mode, the phone maintains the connection to the TLS server indefinitely. If the connection is lost, it begins to reconnect immediately until the connection is established.

If the phone receives a log message during a connection timeout, it discards the messages. The number of log messages lost due to the absence of connection is recorded in a separate local log entry.

You need to configure the following settings for the secure syslog TLS connection:

- ENABLE_PUBLIC_CA_CERTS: specifies whether embedded certificated are trusted or verified against the list defined by TRUSTCERTS.
- TRUSTCERTS: specifies a list of well-known public certificates.
- TLSSRVRID: specifies if the phone performs identity matching for trusted certificates.
- TLS_VERSION: specifies the version of the TLS protocol the phone uses.
- KEYUSAGE_REQUIRED: specifies if key usage extension is checked for.
- LOGSRVR: the value for this parameter must be an FQDN address when you select the secure syslog mode.

You can configure this feature using the `46xxsettings.txt` file, the web user interface and the phone Administrator menu.

Related links

Secure Syslog parameters on page 364

Secure Syslog parameters

Use the following `46xxsettings.txt` file parameters to configure the Secure Syslog feature.

Name	Default value	Description
LOGSRVR_SECURE	0	Specifies if the phone uses secure or non-secure syslog transport mode by default. Value operation: • 0: Non-secure mode using UDP transport • 1: Secure mode using TLS transport RFC 5425 Selected value is available as Default option in Administrator menu

Related links

Secure Syslog on page 364

Geographical restrictions on encryption

Starting from R.4.0.4., SRTP is not supported on Avaya J100 Series IP Phones sold in Russia, Belarus, Kazakhstan, Kyrgyzstan, and Armenia to meet local restrictions on the use of encryption.

On such phones, the settings related to SRTP are excluded both from the phone interface and the web interface, and the administrator cannot enable SRTP.

Chapter 10: SIP server redundancy configuration

SIP server redundancy

In an Open SIP environment, you can configure Avaya J100 Series IP Phones to connect to one of the following SIP servers in a redundant mode.

- Generic open SIP - redundant mode is not supported. However, by connecting to one of the recommended Open SIP servers, you can configure the phone for redundant signaling mode.
- BroadSoft
- Netsapiens

When in redundant mode, the phone uses signaling service from a secondary server if the primary server is down. The following sections explain how to administer a phone for a redundant connection in different modes.

Related links

Redundancy in generic Open SIP on page 366
Redundancy in a Broadsoft environment on page 368
Redundancy in a Netsapiens environment on page 370

Redundancy in generic Open SIP

In a generic Open SIP environment, phone connects to the recommended Open SIP server.

Related links

SIP server redundancy on page 366
Redundancy parameters - generic Open SIP on page 366

Redundancy parameters - generic Open SIP

To configure the phone for redundant signaling mode in a generic Open SIP environment, use the `46xxsettings.txt` file to set the following parameters:

Parameter name	Default value	Required settings
SIPREGPROXYPOLICY	simultaneous	This must be set to alternate.
SIP_CONTROLLERS_LIST_2	Null	This parameter should not be set and left at default. Open SIP redundancy does not support IPv6.
3PCC_SERVER_MODE	0	This parameter should not be set and should be left at default.

SIP_CONTROLLER_LIST	Null	This parameter must be configured to provide redundant sip servers for the phone to connect to.
		It must contain only 2 entries of the following format.
		`host1[:port1] [;transport1=xxx];`
		`host2[:port2] [;transport2=xxx]`
		Host can be an IPV4 address or FQDN. Host cannot be IPV6 address.
		Port and transport values are optional. However, if these values are known, provide them in the settings.
		An example setting:
		`SIP_CONTROLLER_LIST = proxy1.sample.com:tcp:5060;10.10.10.10:tcp:5060`
		Note:
		When SIP_CONTROLLER_LIST contains FQDN, phone uses DNS to resolve the FQDN into IP addresses. If an FQDN resolves to multiple IP addresses, phone uses the first resolved entry.

Set the following parameter when using UDP protocol:

Parameter name	Default value	Recommended settings
REGISTERWAIT	900	This parameter represents number of seconds between register refreshes. It is recommended to set the value to “120” to “180” seconds. This enables faster recovery detection of signaling servers.

Related links

Redundancy in generic Open SIP on page 366

Redundancy in a Broadsoft environment

In a Broadsoft environment, SIP controllers are called application servers. The application servers are deployed as a cluster containing primary and secondary application servers. A cluster is represented as a domain with data replicated between the application servers. The phones use DNS to discover the application servers in the cluster. During DNS lookup operations, DNS returns the sequence of the servers as primary server followed by secondary server.

For more information on the Broadsoft redundancy deployment, see Broadsoft documentation at https://xchange.broadsoft.com/.

Related links

SIP server redundancy on page 366
Redundancy parameters - Broadsoft on page 368

Redundancy parameters - Broadsoft

To configure the phone for redundant signaling mode in a Broadsoft environment use `46xxsettings.txt` file to set the following parameters:

Parameter name	Default value	Required settings
SIPREGPROXYPOLICY	simultaneous	This must be set to alternate.
SIP_CONTROLLERS_LIST_2	Null	This parameter should not be set and left at default. Open SIP redundancy does not support IPv6.
3PCC_SERVER_MODE	0	This parameter should be set to “1”.

Table continues…

Parameter name	Default value	Required settings

SIP_CONTROLLER_LIST	Null	This parameter must be configured to provide redundant sip servers FQDN for the phone to connect to.
		It must contain only 1 entry of the following format.
		`host1[:port1] [;transport1=xxx];`
		Host must be a FQDN. Host cannot be IPV6 address.
		Port and transport values are optional. However, if these values are known, provide them in the settings.
		An example setting:
		`SIP_CONTROLLER_LIST = servers.sample.com:tcp:5060`
		Note:
		When SIP_CONTROLLER_LIST contains FQDN, phone uses DNS to resolve the FQDN into IP addresses. If an FQDN resolves to multiple IP addresses, phone uses the first two resolved entries. If the FQDN resolves to one entry or if the host in SIP_CONTROLLER_LIST contains an IPV4 address, though supported, it is not a redundant signaling configuration.

Set the following parameter when using UDP protocol:

Parameter name	Default value	Recommended settings
REGISTERWAIT	900	This parameter represents number of seconds between register refreshes. It is recommended to set the value to “120” to “180” seconds. This enables faster recovery detection of signaling servers.

Related links

Redundancy in a Broadsoft environment on page 368

Redundancy in a Netsapiens environment

In a Netsapiens environment, you can use up to six SIP controllers in a redundancy deployment. You can use UDP, TCP, or TLS to connect to the SIP controllers.

For more information on the Netsapiens redundancy deployment, see Netsapiens documentation at HTTPS://NETSAPIENS.COM/.

Related links

SIP server redundancy on page 366
Redundancy parameters - Netsapiens on page 370

Redundancy parameters - Netsapiens

To configure the phone for redundant signaling mode in a Netsapiens environment use `46xxsettings.txt` file to set the following parameters:

Parameter name	Default value	Required settings
SIPREGPROXYPOLICY	simultaneous	This must be set to the value alternate.
SIP_CONTROLLERS_LIST_2	Null	This parameter should not be set and left at default. Open SIP redundancy does not support IPv6.
3PCC_SERVER_MODE	0	This parameter should be set to 3.

Table continues…

Parameter name	Default value	Required settings

SIP_CONTROLLER_LIST	Null	This parameter must be configured to provide redundant sip servers FQDN for the phone to connect to.
		It must contain only 1 entry of the following format.
		`host1[:port1] [;transport1=xxx];`
		Host must be a FQDN. Host cannot be IPV6 address.
		Port and transport values are optional. However, if these values are known, provide them in the settings.
		An example setting:
		`SIP_CONTROLLER_LIST = servers.sample.com:tcp:5060`
		When SIP_CONTROLLER_LIST contains FQDN, phone uses DNS to resolve the FQDN into IP addresses. If an FQDN resolves to multiple IP addresses, phone uses the first resolved entries. The number of entries phone uses is determined by MAX_DNS_DISCOVERED_SIP_CONTROLLERS. If the FQDN resolves to one entry or if the host in SIP_CONTROLLER_LIST contains an IPV4 address, though supported, it is not a redundant signaling configuration.

MAX_DNS_DISCOVERED_SIP_CONTROLLERS	2	This parameter specifies the maximum number of the SIP controllers to be used for redundancy from DNS lookup. The value ranges from 2–6 SIP controllers.

Set the following parameter when using UDP protocol:

Parameter name	Default value	Recommended settings
REGISTERWAIT	900	This parameter represents number of seconds between register refreshes. It is recommended to set the value to “120” to “180” seconds. This enables faster recovery detection of signaling servers.

Related links

Redundancy in a Netsapiens environment on page 370

DNS resolution

In the Open SIP modes, phone uses DNS service to lookup a Fully Qualified Domain Name (FQDN) in the host part of SIP_CONTROLLERS_LIST parameter. It uses combination of NAPTR, SRV and a DNS record to resolve a FQDN into prioritized list of **`[IP address, protocol, port]`** set. Administrators must ensure that DNS is configured to return fixed order of servers for the FQDN.

Types of DNS records

The phones use the user domain information and DNS lookups on various DNS records to identify the list of servers and their priority. The phones use a combination of the following DNS records to resolve a user domain into a prioritized list of sets in the format **`[IP address, protocol, port]`**.

- Name Authority Pointer (NAPTR) record: Used to identify the preferred protocol to be used for a specific service. The protocol can be UDP, TCP, or TLS. It provides the information required for the subsequent DNS SRV record lookup. NAPTR record is added to the `devices.avaya.com` domain only if you set the `transport` value of the SET SIP_CONTROLLER_LIST parameter to `auto`. For example:

  ```
  SET SIP_CONTROLLER_LIST "devices.avaya.com;transport=auto"
  ```

- SRV record: Used to identify the list of hosts as FQDNs that provide a service using a specific protocol in a domain. It also provides port information the service is provided at along with the priority of the hosts. SRV lookup provides the list of hosts as FQDNs and the ports used by each host for a service using a protocol.
- A record: Provides a mapping of a host name as a FQDN to an IPV4 address. It also provides the value of time to live (TTL). TTL indicates the duration for which the value can be cached and used by a DNS client.

User experience when redundancy is configured

When the phone is configured for redundant signaling service (primary and secondary servers), it notifies to the user in the following cases:

- There is no signaling service available from either primary or secondary servers. The phone will try to connect these servers and once services from any server are available, the user can log in and the phone becomes available for service.
- Signal delays are encountered on conditions such as the server is busy or the phone is retrying signaling service on a secondary server when the primary is unavailable.

Related links

User interface notification parameter on page 373

User interface notification parameter

Set the following parameter in the `46xxsettings.txt` file to control the UI notification during making a call:

Parameter name	Default value	Description
WAIT_FOR_CALL_OPERATION_RESPONSE	3	Specifies the time in seconds before providing a response for user initiated call operation. **Note:** It is recommended that this parameter should be left to the default value.

Related links

User experience when redundancy is configured on page 373

Chapter 11: Backup and restore

Backup and restore process

Avaya J100 Series IP Phones support the backup and restore of the user-specific data. The phone supports HTTP over TLS (HTTPS) for backup and restore. The following user-specific data are supported for backup and restore:

- User contacts
- Local ring type
- Local Do Not Disturb status
- Local call forward settings
- Auto-answer mode configuration
- Speed dial settings
- Language
- Time zone and time format
- Date format
- PHONEKEY labels

When any user-specific data is modified, the phone automatically backs up the data.

The server gets the extension number of the phone from the backup or restore file name. If an HTTP backup or restore operation requires authentication and the realm matches with the stored realm, the phone uses the stored credentials without prompting the user. When the stored credentials are null, do not match, or authentication fails, the phone displays an HTTP Authentication Failure interrupt screen on the Status or the Prompt Line of the phone with the following message:

`Authentication Failed`

Backup process

The parameter USER_STORE_URI is set with the URI of the backup server in the `46xxsettings.txt` file. If USER_STORE_URI parameter value ends with a / (a forward slash), only the file name is appended. Otherwise, forward slash and file name are both appended to the parameter value. The phone stores the authentication credentials and the realm in volatile memory. If the phone restarts, the phone will prompt you to enter the credentials.

If the authentication with the backup server fails, when a user tries to customize a line key, the phone displays the error `Customization is not available at this time`.

The phone does the following during the backup process:

- Creates a file with all user-specific data.
- Sends the backup file to the server.

If the automatic backup process fails, the phone displays the following message:

`Backup Failed`

Note:

The default value of the credentials and realm is set to null in the following cases:

- At the time of manufacturing.
- When the phone is reset to factory default.
- When user-specific data is removed from the phone.
- Backup process is only initiated when there is a successful retrieval of the user-specific data.

Restore process

- HTTP server requests the file.
- The phone sends the backup file.
- HTTP server returns the file to the phone.

If the automatic restore process fails, the phone displays the following message:

`Retrieval Failed`

Chapter 12: Maintenance

Phone installation - best practices

The phone usually takes a few minutes to boot-up. Depending on your network configuration, you can optimize the boot-up duration by considering the following factors:

- 46xxsettings.txt : The phone parses all the settings that are available in the settings file. Do not use the complete settings file template. Create a new settings file and include only the parameters that you plan to use for the phone. Refer to section Data Privacy on page 362 for details.
- IPv6 : On Avaya J100 Series IP Phones series phones, IPv6 is enabled by default. If your network does not support IPv6, you can disable IPv6 by setting the IPV6STAT to 0 in the `46xxsettings.txt` file.
- 8012.x : Avaya J100 Series IP Phones support IEEE 802.1x parameters. Refer to section Setting the 802.1x operational mode on page 112 for details.
- NTP : On Avaya J100 Series IP Phones the default value of SNTPSRVR server is `0.avaya.pool.ntp.org`. If you are not using the default SNTP servers or if these servers are not reachable, then you can configure the phone with an alternate list of SNTP servers setting the following SNTPSRVR parameter value in the `46xxSettings.txt` file: `"ntp-server-1,ntp-server-2"`, providing IP address or FQDN of the desired NTP server(s). Specifying the correct SNTPSRVR prevents the delay caused by the phone waiting for NTP server timeouts.

Device upgrade process

1. During boot-up, the phone receives the file server address from DHCP, LLDP, or the device interface.
2. The phone contacts the provisioning server to download the firmware upgrade file, `J100Supgrade.txt`.
3. In `J100Supgrade.txt`, the APPNAME parameter contains the firmware version.
4. The phone compares the firmware version specified in the APPNAME parameter with its type.
5. If the firmware version and the phone type match, the phone downloads the files for upgrade.

6. The phone automatically restarts to apply the upgraded firmware.

Periodic check for software and settings update

You can automatically update the phone with the latest software and the settings file. The phone periodically checks for the software and settings update for an automatic update. You can define the frequency, day, date, and time for checking any update files. Whenever there is a new update file, the phone upgrades itself.

The phone performs different actions to apply the following updates:

- When the phone detects a new software, it auto reboots to update.
- When the phone detects settings file parameters that require a reboot, it auto reboots to update the settings.
- When the phone detects a settings file parameters that does not require a reboot, it triggers logout and login of the user to update the settings.
- When the phone detects a new expansion module software, it auto reboots to update to new software.
- When the phone detects resource files such as language files, audio files, image files, contact directory, and certificate, it applies these updates after a manual reboot.

You can define the periodic checks for the software and settings update using the `46xxsettings.txt` file or the Management tab in the web interface.

This feature is not supported in IP office environment.

Related links

Periodic check of software and settings update configuration on page 377

Periodic check of software and settings update configuration

Use the `46xxsettings.txt` file to set the following parameters:

Parameter name	Default value	Description
AUTOMATIC_UPDATE_POLICY	0	Specifies the automatic update frequency. The options are: • 0: Disabled • 1: Daily • 2: Weekly • 3: Monthly This parameter is not supported in IP Office environment.
AUTOMATIC_UPDATE_DAYS	Sun	Specifies the days of automatic update. This parameter is applicable only when AUTOMATIC_UPDATE_POLICY is set to value 2 or 3. Mon, Tue, Wed, Thu, Fri, Sat, Sun for a weekly update. xMon, xTue, xWed, xThu, xFri, xSat, xSun for a monthly update. where x is the occurrence of the month. For example, 2Mon means the second Monday of the month. The phone uses the default value if you set invalid values. Example for weekly update: SET AUTOMATIC_UPDATE_DAYS "Sun" Example for monthly update: SET AUTOMATIC_UPDATE_DAYS "1Sun"

Table continues…

Parameter name	Default value	Description
AUTOMATIC_UPDATE_WINDOW	2,4	Specifies the window for the automatic update of the phone. Value m, n specifies the hours to Start and End the window for automatic update, where m, n are numeric values ranging from 0 to 23. For example, 3,4 means the automatic update Starts and Ends between 3 a.m. and 4 a.m. Each phone picks a random time between this specified window. The time is in 24hr format. Few examples, SET AUTOMATIC_UPDATE_WINDOW "23,0". Sets 1 hour window from 11 p.m. to 00 a.m. next day for the automatic update. For "22,2". Sets 4 hour window from 10 p.m. to 2 a.m. next day for the automatic update. For "0,0". Sets 24 hour window from 00 a.m. to 00 a.m. next day for the automatic update. For "0,1". Sets 1 hour window from 00 a.m. to 1 a.m. for the automatic update.

Table continues…

Parameter name	Default value	Description
AUTOMATIC_UPGRADE_INSTALL_DATE_TIME	Null	Specifies the date and time after which the new firmware is downloaded and installed. After this date and time is reached, the phone uses the settings of AUTOMATIC_UPDATE_DAYS and AUTOMATIC_UPDATE_WINDOW to trigger firmware download reboot. If this parameter value is not set, the phone uses AUTOMATIC_UPDATE_POLICY, AUTOMATIC_UPDATE_DAYS, and AUTOMATIC_UPDATE_WINDOW to trigger the firmware download. AUTOMATIC_UPGRADE_INSTALL_DATE_TIME is applicable if AUTOMATIC_UPDATE_POLICY is set to 1, 2, or 3. The format is YYYY-MM-DDThh:mm, where: • YYYY is a 4 digit numeric value for the year, MM is a 2 digit numeric value for the month • DD is a 2 digit numeric value for the date, which is 1 to 31 • T is the time separator • hh is a 2 digit numeric value for hours of the day which is 00 to 23 • mm is a 2 digit numeric value for minutes of the hour, which is 00 to 59 For example, SET AUTOMATIC_UPGRADE_INSTALL_DATE_TIME 2015-04-12T23:20 Note that this parameter applies to the local time of the phone as defined by the following parameters: • GMTOFFSET • DAYLIGHT_SAVING_SETTING_MODE • DSTOFFSET • DSTSTART • DSTSTOP

Table continues…

Parameter name	Default value	Description
AUTOMATIC_UPDATE_REBOOT_PROMPT	0	Specifies if the user is prompted for confirmation when the phone detects a new software update that requires a reboot. Reboot is triggered immediately for configuration changes that require a reboot. Update policy parameters such as AUTOMATIC_UPDATE_POLICY, AUTOMATIC_UPDATE_DAYS, AUTOMATIC_UPDATE_WINDOW, and AUTOMATIC_UPGRADE_INSTALL_DATE_TIME are updated without a reboot. The options are: • 0: The phone does not display the reboot confirmation prompt. Instead it updates the phone directly. • 1: The phone displays the reboot confirmation prompt.

For example, to auto update the settings every Sunday of the month, and auto upgrade the firmware on 1st Sunday of every month after 1 Feb 2021, set the following parameters:

- SET AUTOMATIC_UPDATE_POLICY 2
- SET AUTOMATIC_UPDATE_DAYS "Sun"
- SET AUTOMATIC_UPDATE_WINDOW "7,10"
- SET AUTOMATIC_UPGRADE_INSTALL_DATE_TIME "2021-02-01T12:12"

Related links

Periodic check for software and settings update on page 377

Avaya J100 Expansion Module upgrade

You can upgrade the Avaya J100 Expansion Module firmware to a new version using Avaya J100 Series IP Phones software distribution package. The combined package includes `.bin` files for the button module upgrade, for example: `FW_JEM24_R1_0_1_0_9.bin`.

In the `J100Supgrade.txt` file, the following parameter points at the Avaya J100 Expansion Module upgrade file:

```
SET JEM24_APPNAME FW_JEM24_R1_0_1_0_9.bin
```

During the boot-up, the phone downloads the new firmware for the Avaya J100 Expansion Module. The phone screen displays `Updating software` notification.

After the phone downloads the expansion module firmware, the upgrade process continues in the background. On the phone screen navigate to **Main Menu** > **Administration** > **View** > **Button modules**, to see the **Upgrading** status.

During the upgrade procedure, the Avaya J100 Expansion Module is functional. You can access functionalities such as make and receive calls. Each module attached to the phone takes up to four hours to upgrade from an older software version to 1.0.1, and it takes up to an hour and a half to upgrade from software version 1.0.1 to a new one.

When the upgrade is complete, the Avaya J100 Expansion Module displays the following notification: "`This device will be out of service for 3 minutes to apply the update. It will be applied automatically between 12am and 3am.`". Press the corresponding line button for **Apply now** or **Apply tonight** option to select the suitable upgrade time.

Note:

When the phone screen displays the Upgrade notification, the phone disables the expansion module screen saver and does not turn off the backlight.

Upgrading the expansion module

About this task

Use this task to upgrade Avaya J100 Expansion Module firmware to a new version.

Before you begin

Download Avaya J100 Series IP Phones software distribution package from the Avaya support website.

Procedure

1. Extract the zipped file with the expansion module firmware and save it at an appropriate location on the file server.
2. Set the expansion module firmware file name in `J100Supgrade.txt`.
3. Reboot the phone. The expansion module will reboot automatically.

Post installation checklist

To ensure that the phone is properly installed and running properly, verify that the following requirements are complete.

No.	Task	Reference	✔
1	Has the phone acquired an IP address?		

Table continues…

No.	Task	Reference	✔
2	Are you able to make a call from the phone?		
3	Are you able to perform backup-restore?		
3	Are you able to modify the phone's Settings file parameters and end user settings.	Configuration parameters on page 387	
4	Are you able to upgrade your phone?	Device upgrade process on page 376	
5	Have you installed the appropriate private network authentication certificates?		

Chapter 13: Resources

Documentation

Title	Use this document to:	Audience
Installing and Administering		
Installing and Administering Avaya J100 Series SIP IP Phones in Open SIP	See information about preparing Avaya J100 Series IP Phones for installation, deployment, initial administration, and administration tasks including data and security.	For people who want to install, administer, and maintain Avaya J100 Series IP Phones.

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.
7. Click **Enter**.

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.

- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.

- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** ( ).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:

  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.

- Add yourself as a watcher using the **Watch** icon ( ).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:

  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Appendix A: Customizable parameters

List of configuration parameters

Parameter name	Default value	Description
100REL_SUPPORT	1	Specifies whether the 100rel option tag is included in the **SIP INVITE** header field. Value operation: • 0: Not included. • 1: Included.
3PCC_SERVER_MODE	0	Specifies the server mode. Value operation: • 0: Generic • 1: BroadSoft • 3: Netsapiens • 5: ACO, Avaya J129 IP Phone does not support this value. **Note:** Value 4 is not supported from firmware version 4.0.8 onwards. Starting from firmware version 4.0.8, use value 5 to connect to the RingCentral® server. Value 5 supports both RCO and ACO.
A		

Table continues…

Parameter name	Default value	Description
ACOUSTIC_EXPOSURE_PROTECT_MODE_DEFAULT	Off	Specifies the long-term acoustic exposure protection mode default setting. Value operation: • Off • Dynamic: • 4 hours • 8 hours **Note:** Avaya J129 IP Phone does not support long-term acoustic exposure protection.
ADMIN_LOGIN_ATTEMPT_ALLOWED	10	Specifies the allowed number of failed attempts for accessing the **Admin** menu.
ADMIN_LOGIN_LOCKED_TIME	10	Specifies the duration for lockout when a user reaches the maximum attempts limit for accessing the **Admin** menu. Valid values are from 5 min to 1,440 min.
ADMIN_PASSWORD	27238	Specifies an access code for accessing the **Admin** menu. Valid values are from 6 to 31 alphanumeric characters. **Note:** If this parameter length is set below 6 or above 31 alphanumeric characters, then the parameter is treated as not defined.
ADMINTIMEFORMAT	0	Specifies whether TIMEFORMAT value is forced or a user can change the time format in user interface. Value operation: • 0: AM/PM format, user can change time format. • 1: 24 hour format, user can change format. • 2: forced AM/PM format. • 3: forced 24 hour format. **Note:** IP Office CCMS environment does not support this parameter.

Table continues…

Parameter name	Default value	Description
AGCHAND	1	Specifies the status of Automatic Gain Control (AGC) for the handset. Value operation: • 0: Disables AGC for the handset. • 1: Enables AGC for the handset.
AGCHEAD	1	Specifies the status of Automatic Gain Control (AGC) for the headset. Value operation: • 0: Disables AGC for the headset. • 1: Enables AGC for the headset.
AGCSPKR	1	Specifies the status of Automatic Gain Control (AGC) for the speaker. Value operation: • 0: Disables AGC for the speaker. • 1: Enables AGC for the speaker.
ALLOW_BLF_LIST_CHANGE	3	Specifies whether a user can add or delete the monitored phone extensions from the BLF resource list. **Note:** This parameter is supported only in the Broadworks environment. Avaya J129 IP Phone does not support this feature. Value operation: 0: The user cannot add or delete monitored phone extensions. 1: The user can only delete monitored phone extensions. 2: The user can only add monitored phone extensions. 3: The user can add and delete monitored phone extensions.

Table continues…

Parameter name	Default value	Description
APPLICATION_HEADER_APPEARANCE_CONTEXT	0	Specifies whether appearances context will be shown on the Application Header Line in Phone List View. When idle the line can optionally display the user configured SHORT_FORM_USER_ID and DISPLAY_NAME to display the Application Header line context appropriately. Value operation: 0 -appearances context is not be shown on the Application Header Line (default) 1 -appearances context will be shown on the Application Header Line for various states, including name of the shared line key or BLF key, when applicable. 2 -appearances context will be shown on the Application Header Line for various states, including name of BLF key, when applicable. **Note:** Avaya J129 IP Phone does not support this parameter.
AUDASYS	3	Specifies the audible alerting setting for the phone. Value operation: • 0: Turns off audible alerting. User cannot adjust ringer volume. • 1: Turns on audible alerting. User can adjust ringer volume, but cannot turn off audible alerting. • 2: Turns off audible alerting. User can adjust ringer volume and can turn off audible alerting. • 3: Turns on audible alerting. User can adjust ringer volume and can turn off audible alerting. **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
AUDIOENV	0	Specifies the audio environment index and enables you to customize the phone's audio performance. Valid values are 0 through 299. This parameter affects settings for AGC dynamic range and handset noise reduction thresholds. Always consult Avaya before changing this parameter.
AUDIOPATH_DEFAULT	1	Specifies the audio path for the phone. Only if you set the value to 1 or 2, the user can change the audio path from the phone UI. Value operation: • 1: Speaker • 2: Headset • 3: Speaker forced • 4: Headset forced
AUDIOSTHD	0	Specifies the level of side-tone in the headset. Value operation: • 0: Normal • 1: Softer by one level. • 2: Softer by two levels. • 3: Softer by three levels. • 4: OFF. • 5: Louder by one level.

Table continues…

Parameter name	Default value	Description
AUDIOSTHS	0	Specifies the level of side-tone in the handset. Value operation: • 0: Normal • 1: Softer by three levels. • 2: OFF. • 3: Softer by one level. • 4: Softer by two levels. • 5: Softer by four levels. • 6: Softer by five levels. • 7: Softer by six levels. • 8: Louder by one level. • 9: Louder by two levels.
AUTH	0	Specifies if the script files are to be downloaded from an authenticated server over an HTTPS link. Value operation: • 0: Optional • 1: Mandatory To revert the configured value of 1 to the default one, reset the phone to defaults.
AUTHCTRLSTAT	0	Specifies that the enhanced debugging capabilities are activated from an SSH server by an AVAYA engineer. Value operation: • 0: Enhanced debugging capabilities are disabled. • 1: Enhanced debugging capabilities are enabled. **Note:** The parameter must be set to 1 only for the debugging period. Set the parameter back to 0 when debugging is complete.

Table continues…

Parameter name	Default value	Description
AUTO_ANSWER_DURING_CALL	0	Specifies auto-answer calls during another active call. Value operation: • 0: Do not auto-answer when there is an active call • 1: Auto-answer when there is an active call **Note:** Avaya J129 IP Phone does not support this feature.
AUTO_ANSWER_MUTE_ENABLE	1	Specifies the status of the mute function for the auto-answered calls. Value operation: • 0: Disabled • 1: Enabled
AUTO_SELECT_ANY_IDLE_APPR BLF_LIST_URI	0	Specifies that any idle call appearance (primary or bridged) can be automatically selected. This parameter works along with the parameter CONF_TRANS_ON_PRIMARY_APPR. Value operation: • 0: Disabled. Both parameters AUTO_SELECT_ANY_IDLE_APPR and AUTO_SELECT_ANY_IDLE_APPR are set to 0. • 1: Enabled. The parameter CONF_TRANS_ON_PRIMARY_APPR is set to 0. **Note:** Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description
AUTOMATIC_UPDATE_DAYS	Sun	Specifies the days of automatic update. This parameter is applicable only when AUTOMATIC_UPDATE_POLICY is set to value 2 or 3. Mon, Tue, Wed, Thu, Fri, Sat, Sun for weekly update. xMon, xTue, xWed, xThu, xFri, xSat, xSun for monthly update. where x is the occurrence of the month. For example: 2Mon, means second Monday of the month. The phone uses the default value if you set invalid values. Example for weekly update SET AUTOMATIC_UPDATE_DAYS "Sun" Example for monthly update SET AUTOMATIC_UPDATE_DAYS "1Sun"

Table continues…

Parameter name	Default value	Description
AUTOMATIC_UPGRADE_INSTALL_DATE_TIME	Null	Specifies the date and time after which the new firmware is downloaded and installed. After this date and time is reached, the phone uses the settings of AUTOMATIC_UPDATE_DAYS and AUTOMATIC_UPDATE_WINDOW to trigger firmware download reboot. If this parameter value is not set, then the phone uses AUTOMATIC_UPDATE_POLICY, AUTOMATIC_UPDATE_DAYS, and AUTOMATIC_UPDATE_WINDOW to trigger the firmware download. AUTOMATIC_UPGRADE_INSTALL_DATE_TIME is applicable if AUTOMATIC_UPDATE_POLICY is set to 1, 2, or 3. The format is YYYY-MM-DDThh:mm, where: • YYYY is 4 digit numeric value for year, MM is 2 digit numeric value for month • DD is 2 digit numeric value for date, which is 1 to 31 • T is the time separator • hh is 2 digit numeric value for hours of the day which is 00 to 23 • mm is 2 digit numeric value for minutes of the hour, which is 00 to 59 For example: SET AUTOMATIC_UPGRADE_INSTALL_DATE_TIME 2015-04-12T23:20 Note that this parameter applies to the phone local time as defined by the following parameters: • GMTOFFSET • DAYLIGHT_SAVING_SETTING_MODE • DSTOFFSET • DSTSTART • DSTSTOP

Table continues…

Parameter name	Default value	Description
AUTOMATIC_UPDATE_REBOOT_PROMPT	0	Specifies if the user is prompted for confirmation when the phone detects a new software update that requires a reboot. Reboot is triggered immediately for configuration changes that require a reboot. Update policy parameters such as AUTOMATIC_UPDATE_POLICY, AUTOMATIC_UPDATE_DAYS, AUTOMATIC_UPDATE_WINDOW, and AUTOMATIC_UPGRADE_INSTALL_DATE_TIME are updated without a reboot. Value operation: • 0: The phone does not display the reboot confirmation prompt, instead it updates the phone directly. • 1: The phone displays the reboot confirmation prompt.
AUTOMATIC_UPDATE_POLICY	0	Specifies the automatic update frequency. Value operation: • 0: Disabled • 1: Daily • 2 : Weekly • 3: Monthly
AUTOMATIC_UPDATE_WINDOW	2,4	Specifies the window for the automatic update of the phone. Value m, n specifies the hours to Start and End the window for automatic update, where m, n are numeric values ranging from 0 to 23. For example, 3,4 means the automatic update Starts and Ends between 3 AM and 4 AM. Each phone picks a random time between this specified window. The time is in 24hr format. For example SET AUTOMATIC_UPDATE_WINDOW "23,0" Sets one hour window from 11 PM to 00 AM for the automatic update.

Table continues…

Parameter name	Default value	Description
AWAY_TIMER	1	Specifies whether the phone must report an away state. Value operation: • 0: Disabled. • 1: Enabled.
AWAY_TIMER_VALUE	30	Specifies the number of minutes of idle time after which the phone assumes that the user is away from the phone. Valid values are from 1 to 1500 minutes.
B		
BACKGROUND_IMAGE	Null	Specifies custom background images that can be loaded from the provisioning server. Phone supports up to 5 background images with the following limitation: • Only jpeg format files are supported. • The maximum file size is 256 KB. • The file names are case sensitive. Avaya J169/J179 IP Phone, Avaya J159 IP Phone, and Avaya J139 IP Phonescreen resolution is 320 pixels x 240 pixels. Avaya J169/J179 IP Phone, Avaya J189 IP Phone color depth is 16 bits. The files shall be stored in the same directory defined by HTTPDIR / TLSDIR. Example: SET BACKGROUND_IMAGE [xxx.jpg]
BACKGROUND_IMAGE_DISPLAY	Null	Specifies the background image to be displayed. **Note:** If BACKGROUND_IMAGE_SELECTABLE is set to 1, the end user may override this setting. **Note:** Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description
BACKGROUND_IMAGE_SELECTABLE	1	Allows the end user to select background images. Value operation: • 0: The user can not use a background images from the phone UI. • 1: The user can select a background images from the phone UI. **Note:** Avaya J129 IP Phone does not support this feature.
BACKGROUND_IMAGE_SECONDARY	Null	Specifies a list of background images to be used on the secondary screen. Phone supports up to 5 background images with the following limitation: • Only jpeg format files are supported. • The maximum file size is 256 KB. • The file names are case sensitive. Example: background_example1.jpg,background_example2.jpeg **Note:** This parameter is supported only in Avaya J159 IP Phone
BACKGROUND_IMAGE_DISPLAY_SECONDARY	Null	Specifies the background image to be displayed on the Secondary screen. The filename will be one of the filenames listed in BACKGROUND_IMAGE_SECONDARY. Note that if BACKGROUND_IMAGE_SELECTABLE_SECONDARY is set to 1 then the end user may override this setting.

Table continues…

Parameter name	Default value	Description
BACKGROUND_IMAGE_SELECTABLE_SECONDARY	1	Allows the end user to select background images for the secondary screen. Value operation: • 0: The user can not use a background images from the phone UI. • 1: The user can select a background images from the phone UI. This parameter overrides the value configured using BACKGROUND_IMAGE_DISPLAY_SECONDARY parameter **Note:** This parameter is supported only in Avaya J159 IP Phone
BACKLIGHT_SELECTABLE	0	Specifies whether backlight timer is selected by the administrator (BAKLIGHTOFF) or user. Value operation: • 0: To set Backlight Timer value from `46xxsettings` file. • 1: To set Backlight Timer value according to user settings. **Note:** Avaya J129 IP Phone does not support this feature.
BEACON_INDICATION_MODE	0	Specifies the behavior of a Beacon LED at an incoming call. Applies to primary, shared, BLF and BLF park lines. Value operation: • 0: Beacon LED flashes immediately, when there is an incoming call and until call is answered. • 1: Beacon LED flashes after a delay as per delayed ringing configuration, when there is an incoming call and until call is answered or ignored.

Table continues…

Parameter name	Default value	Description
BLF_LIST_URI	None	Specifies a unique name for the BLF list of users that you want to monitor on the phone. See BLF parameters on page 274 for more details. **Note:** Avaya J129 IP Phone does not support this feature.
BLF_LIST_PREFERRED_START_LOCATION	0	Specifies where the phone places detected BLFs on the home screen. The phone detects BLFs from BLF List URI. It provides the starting location from which the detected BLFs are placed. Valid values are 0 through 96. **Note:** This parameter is supported only in the Broadworks and Asterisk environment. Valid values: 0 –BLFs will be placed depending on Button Module detection. Starting location is 1 if no BM. Starting location is 25 if a button module is detected on the phone. 1-96 – Specifies the precise line key number.
BLF_LIST_LINEKEY_LOCATION_FORCED	1	Specifies if BLF line key placement is forced or not. When forced, the user cannot move, delete or relabel BLF line keys. **Note:** This parameter is supported only in the Broadworks and Asterisk environment. Valid values: 0 – Non-forced 1 – Forced It is recommended to use forced value for this parameter.

Table continues…

Parameter name	Default value	Description
BLF_INCOMING_CALL_INDICATION	3	Specifies the indication type for a BLF incoming call. Valid values: • 0 - None (no alerting for BLF incoming calls). • 1 - Audible (only audible alerting for BLF incoming calls). • 2 - Visual (only visual alerting for BLF incoming calls). • 3 - Default (the behavior isl based on BLF_INCOMING_CALL_INDICATION_MODE parameter value). • 4 - Both (both audible and visual alerting for BLF incoming calls). **Note:** This parameter is supported only in the 3PCC environment. Avaya J129 IP Phone does not support this feature.
BLF_PARKED_CALL_INDICATION	1	Specifies the indication type for a BLF parked call. Valid values: • 0 - None (no alerting for BLF parked calls). • 1 - Default (the behavior based on BLF_PARKED_CALL_INDICATION_MODE parameter value). • 2 - Audible (only audible alerting for BLF parked call). • 3 - Visual (only visual alerting for BLF parked call). • 4 - Both (default - both audible and visual alerting for BLF parked call). **Note:** This parameter is supported only in the 3PCC environment. Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description
BLF_INCOMING_CALL_INDICATION_MODE	3	Specifies the indication mode for a BLF incoming call. Valid values: • 0 - None (no alerting for BLF incoming call). • 1 - Audible (only audible alerting for BLF incoming call). • 2 - Visual (only visual alerting for BLF incoming call). • 3 - Both (both audible and visual alerting for BLF incoming call) • 4 - Force None (forced only audible alerting for BLF incoming call). • 5 - Force Audible (forced only audible alerting for BLF incoming call). • 6 - Force Visual (forced only visual alerting for BLF incoming call). • 7 - Force Both (forced both audible and visual alerting for BLF incoming call). **Note:** This parameter is supported only in the 3PCC environment. Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description
BLF_PARKED_CALL_INDICATION_MODE	1	Specifies the indication move for a BLF parked call. Valid values: • 0 - None (no alerting for BLF parked call). • 1 - Audible (only audible alerting for BLF parked call). • 2 - Visual (only visual alerting for BLF parked call). • 3 - Both (both audible and visual alerting for BLF parked call) • 4 - Force None (forced only audible alerting for BLF parked call). • 5 - Force Audible (forced only audible alerting for BLF parked call). • 6 - Force Visual (forced only visual alerting for BLF parked call). • 7 - Force Both (forced both audible and visual alerting for BLF parked call). **Note:** This parameter is supported only in the 3PCC environment.
BLF_PICKUP_METHOD	0	Specifies whether pickup BLF call is using Invite with FAC in Request URI or using Invite with Replaces header. Value operation: • 0: Pickup BLF call using Invite with FAC in Request URI • 1: Pickup BLF call using Invite with Replaces header **Note:** This parameter is available in • Avaya J139 IP Phone • Avaya J159 IP Phone • Avaya J169/J179 IP Phone

Table continues…

Parameter name	Default value	Description
BLOCK_CERTIFICATE_WILDCARDS	0	Specifies whether the endpoint will accept server identity certificates with wildcards. Value operation: • 0: Accept wildcards in certificate. • 1: Do not accept wildcards in certificates.
BLUETOOTHSTAT	1	Specifies whether the user is given an option to enable the Bluetooth. Value operation: • 0: Bluetooth is disabled and the user is not given an option to enable it. • 1: The user is given an option to enable the bluetooth (default).
BRANDING_VOLUME	5	Specifies the volume level at which the Avaya audio brand is played. Value operation: • 8: 9db above nominal • 7: 6db above nominal • 6: 3db above nominal • 5: nominal (default) • 4: 3db below nominal • 3: 6db below nominal • 2: 9db below nominal • 1: 12db below nominal • 0: No volume
BRURI	Null	Provides the capability to send a phone report to a server with the URI of the server defined by this parameter. To send the report, go to **Main Menu** > **Admin** > **Debug** > **Phone report**.

Table continues…

Parameter name	Default value	Description
BS_CC_ENABLED	0	Specifies if the Broadsoft Call Center needs to be enabled on the phone. This parameter is used only if XSI is disabled (XSI_URL is empty). Options are: • 0: To disable the parameter. • 1: To enable the parameter. **Note:** Avaya J129 IP Phone does not support this feature.
BS_CC_UNAVAIL_CODES	Null	Specifies codes that can be selected when an agent selects Unavailable state. This parameter is used only if XSI is disabled (XSI_URL is empty). You can enter the comma separated list of the reason codes and their descriptions as shown here: code = description, example: 1= coffee break, 2= Tea party, dnd= Do Not Disturb **Note:** Avaya J129 IP Phone does not support this feature.
BS_CC_AUTOMATIC_STATE	0	Specifies if the phone automatically changes the agent state during logging in and logging out. Options are: • 0: To disable the parameter. • 1: To enable the parameter. **Note:** Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description
BS_CC_DISP_CODES	Null	Specifies call dispositions codes that the call center agents can apply to a call center call. You can enter comma separated string values of disposition codes. For example: 1=Follow-up required, sales:2=New customer, helpdesk:3=Issue resolved; 4=Issue unresolved , meaning 1 is available for all call centers, 2 is specific for sales and 3 and 4 are specific for helpdesk This parameter is used only if XSI_URL is empty. **Note:** Avaya J129 IP Phone does not support this feature.
BS_CC_SUPERVISORS	Null	Specifies supervisors whom the call center agents can call to. You can enter comma separated string values of supervisors. For example : 6551=Supervisor1, sales:6552=Supervisor2, helpdesk:6553=Supervisor3; 6554=Supervisor4, meaning 6551 is available for all call centers, 6552 is specific for sales and 6553 and 6554 are specific for helpdesk This parameter is used only if XSI_URL is empty. **Note:** Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description
BUTTON_MAPPINGS	Null	Specifies a list of Button and Status pairs that change the operation of some of the buttons on the phone. Button and 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 is disabled. • cc-release: Button invokes the cc-release feature. • null: All buttons operate normally.
BW_ENABLE_DIR	1	Specifies if directory contacts are available for processing. Value operation: • 0: Directory contacts are not processed and directory sources are not displayed to the user. • 1: Directory contacts are processed and directory sources are displayed to the user. **Note:** Avaya J129 IP Phone does not support this feature.
BW_ENABLE_DIR_ENTERPRISE	1	Specifies if Enterprise directory contacts are available for processing. Value operation: • 0: Enterprise directory contacts are not processed. • 1: Enterprise directory contacts are processed.
BW_ENABLE_DIR_ENTERPRISE_COMMON	1	Specifies if Enterprise common directory contacts are available for processing. Value operation: • 0: Enterprise common directory contacts are not processed. • 1: Enterprise common directory contacts are processed.

Table continues…

Parameter name	Default value	Description
BW_ENABLE_DIR_GROUP	1	Specifies if Group contacts are available for processing. Value operation: • 0: Group contacts are not processed. • 1: Group contacts are processed. **Note:** Avaya J129 IP Phone does not support this feature.
BW_ENABLE_DIR_GROUP_COMMON	1	Specifies if Group Common contacts are available for processing. Value operation: • 0: Group common contacts are not processed. • 1: Group common contacts are processed. **Note:** Avaya J129 IP Phone does not support this feature.
BW_ENABLE_DIR_PERSONAL	1	Specifies if Personal contacts are available for processing. Value operation: • 0: Personal contacts are not processed. • 1: Personal contacts are processed. **Note:** Avaya J129 IP Phone does not support this feature.
BW_ENABLE_DIR_CUSTOM	1	Specifies BroadWorks Custom directory availability state. Value operation: • 0: disabled. • 1: enabled. **Note:** Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description
BW_DIR_ENTERPRISE_DESCRIPTION	“Enterprise”	Specifies the display name for Enterprise directory. **Note:** Avaya J129 IP Phone does not support this feature.
BW_DIR_ENTERPRISE_COMMON_DESCRIPTION	“Enterprise Common”	Specifies the display name for Enterprise Common directory. **Note:** Avaya J129 IP Phone does not support this feature.
BW_DIR_GROUP_DESCRIPTION	“Group”	Specifies the display name for Group directory. **Note:** Avaya J129 IP Phone does not support this feature.
BW_DIR_GROUP_COMMON_DESCRIPTION	“Group Common”	Specifies the display name for Group Common directory. **Note:** Avaya J129 IP Phone does not support this feature.
BW_DIR_PERSONAL_DESCRIPTION	“Personal”	Specifies the display name for Personal directory. **Note:** Avaya J129 IP Phone does not support this feature.
BW_DIR_CUSTOM_DESCRIPTION	“Custom”	Specifies the display name for Custom directory. **Note:** Avaya J129 IP Phone does not support this feature.
BW_DIR_ENTERPRISE_EXTENSION	"BWEntr"	Specifies the display name for Enterprise directory extension. **Note:** Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description
BW_DIR_ENTERPRISE_COMMON_EXTENSION	"BW EnCom"	Specifies the display name for Enterprise Common directory extension. **Note:** Avaya J129 IP Phone does not support this feature.
BW_DIR_GROUP_EXTENSION	"BW Group"	Specifies the display name for Group directory extension. **Note:** Avaya J129 IP Phone does not support this feature.
BW_DIR_GROUP_COMMON_EXTENSION	"BW GrCom"	Specifies the display name for Group Common directory extension. **Note:** Avaya J129 IP Phone does not support this feature.
BW_DIR_PERSONAL_EXTENSION	"BW Pers"	Specifies the display name for Personal directory extension. **Note:** Avaya J129 IP Phone does not support this feature.
BW_DIR_CUSTOM_EXTENSION	"BW Cust"	Specifies the display name for Custom directory extension. **Note:** Avaya J129 IP Phone does not support this feature.
C		

Table continues…

Parameter name	Default value	Description
CALL_DECLINE_POLICY	0	Specifies whether the user can decline the incoming call. You can enable and disable the feature using the following options: The options are: • **0**: The feature is disabled, the **Decline** soft key does not appear on the phone screen for an incoming call. This is the default value. • **1**: 486 method is used. By selecting this value you enable the Call decline policy for the user. 486 method indicates that the call ringing location is not available to take the call. However, the ringing continues in other locations. • **2**: 603 method is used. By selecting this value you enable the Call decline policy for the user. 603 method indicates that no location is available to take the call.
CALL_FORWARD_DELAY_USER	0	Specifies the number of rings after which a call will be forwarded if it remains unanswered. Valid values are 0–20. If you select 0 the value of the CALL_FORWARD_DELAY will be used
CALL_TRANSFER_MODE	0	Determines the call transfer mode in an Open SIP environment. Valid value is 0 or 1.

Table continues…

Parameter name	Default value	Description
CALLFWDSTAT	0	Sets the call forwarding mode of the phone by summing following the values: • 0: Disables call forwarding. • 1: Permits unconditional call forwarding. • 2: Permits call forward on busy. • 3: Permits call forward on busy and unconditional call forwarding. • 4: Permits call forward/no answer. • 5: Permits call forward/no answer and unconditional call forwarding. • 6: Permits call forward/no answer and call forward on busy. • 7: Permits call forward/no answer and call forward on busy and unconditional call forwarding.
CALLFWD_CHAIN_ORDER	0	The "Forwarded by" details that are shown for incoming calls that have been forwarded by another user. Specifies which user information to be displayed on an incoming call if there are multiple forwards before being received as an incoming call. Value operations: • 0: First user to have forwarded is shown as the Forwarded By User. • 1: Last user to have forwarded is shown as the Forwarded By User. **Note:** Avaya J129 IP Phone does not support this feature.
CALL_PICKUP_BARGEIN_FAC	*33	Specifies the feature access code of Directed Call Pickup with Barge-In. **Note:** Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description
CALL_PICKUP_FAC	*97	Specifies the feature access code of Directed Call Pickup to pick up a call for a BLF user. **Note:** Avaya J129 IP Phone does not support this feature.
CALL_PARK_FAC	Null	Specifies FAC used to make a park operation by calling CALL_PARK_FAC followed by a destination number. This parameter is required when the shortcut action for Active call shortcut keys feature is set to Park (4). **Note:** Avaya J129 IP Phone does not support this feature.
CALL_PARK_DYNAMIC_METHOD	0	Specifies the method the phone will use to park an active call to a dynamic parking slot assigned by the server. Value operation: • 0: Blind Transfer: the active call is blind transferred to the CALL_PARK_DYNAMIC_FAC (Default) • 1: DTMF: provide the CALL_PARK_DYNAMIC_FAC digits into the active call **Note:** Avaya J129 IP Phonedoes not support this parameter.
CALL_PARK_DYNAMIC_FAC	Null	Specifies the Feature Access Code that the phone will use to park an active call to a dynamic parking slot assigned by the server. **Note:** Avaya J129 IP Phonedoes not support this parameter.
CALL_PAGE_EXTENSION_FAC	Null	Specifies the Page feature access code that is used to inform the server to perform a page to an extension. **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
CALL_PAGE_GROUP_FAC	Null	Specifies the Page feature access code that is used to inform the server to perform a page to an extension. **Note:** Avaya J129 IP Phonedoes not support this parameter.
CALL_PAGING_GROUPS	Null	Specifies a comma separated list of paging groups a user is allowed to call (PagingGroupLabel:PagingGroupAddress). "PagingGroupLabel" is a string describing the PagingGroupAddress. "PagingGroupAddress" is the address/ number of the PagingGroupLabel. This parameter is used by ENABLE_PARK_AND_PAGE feature and displays the user a list of the PagingGroups when performing Park and Page. "PagingGroupLabel" up to 32 unicode chars. "PagingGroupAddress" up to 64 alphanumeric chars, an extension, an address or sip uri. PagingGroupLabel and PagingGroupAddress can not contain: ;",=|<>/&,
CALL_UNPARK_FAC	*88	Specifies the feature access code to unpark a call for a BLF user. **Note:** This parameter is supported only in the Broadworks environment. **Note:** Avaya J129 IP Phone does not support this feature.
CC_INFO_TIMER	8	Specifies the duration, in hours, of the subscription to the SIP CC-Info event package. Valid values are 1 through 24.

Table continues…

Parameter name	Default value	Description
CERT_WARNING_DAYS	60	Specifies the number of days before the expiration of a certificate that a warning will first appear on the phone screen. Certificates include trusted certificates, OCSP certificates and identity certificate. Log and Syslog message will also be generated. The warning will reappear every seven days.Valid values are from 0 to 99. Value operation: • 0: No certificate expiration warning will be generated.
CERT_WARNING_DAYS_EASG	365	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 also generated. Valid values are from 90 to 730.
CLDISPCONTENT	1	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. **Note:** Avaya J129 IP Phone and Avaya J139 IP Phonedo not support this feature.

Table continues…

Parameter name	Default value	Description
CONF_TRANS_ON_PRIMARY_APPR	0	Determines conference and transfer setup whether to use idle primary call appearance or idle bridged call appearance. Value operation: • 0: To specify conference and transfer setup to use an idle primary call appearance at first attempt. However, if an idle primary call appearance is unavailable, then the setup will use idle bridged call appearance regardless of the setting of AUTO_SELECT_ANY_IDLE_APPR. If a bridged call appearance initiates the setup, then setup will use idle bridged call appearance of same extension. If an idle bridged call appearance of the same extension is not available and AUTO_SELECT_ANY_IDLE_APPR is set to 1, then setup will use any idle call appearance. However, if AUTO_SELECT_ANY_IDLE_APPR is set to 0 and if same bridged call extension is not available, the setup initiated on a bridged call appearance will be denied. • 1: To specify conference and transfer setup to use an idle primary call appearance at first attempt. However, if an idle primary call appearance is unavailable, then the setup will use idle bridged call appearance. If a bridged call appearance initiates the setup, then setup will use idle bridged call appearance of either the same extension or different extension. AUTO_SELECT_ANY_IDLE_APPR is ignored. **Note:** Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description
CONFERENCE_FACTORY_URI	Null	Specifies the URI for conference for Network Conferencing in an Open SIP environment. Valid values contain zero or one URI, where a URI consists of a dial string followed by @, and then the domain name, which must match the routing pattern configured in System Manager for Adhoc Conferencing. Depending on the dial plan, the dial string can 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.
CONFERENCE_TYPE	1	Determines the selection of the Conference Method. Value operation: • 0: Local conferencing is supported based on sipping services. • 1: Server based conferencing is supported. • 2: Click-to conference server based conferencing is supported. If the parameter is set to a value that is outside the range then default value is selected. **Note:** The parameter is set to 0 in IP Office environment.
CONFIG_SERVER_SECURE_MODE	1	Specifies whether HTTP or HTTPS is used to access the configuration server. Value operation: • 0: HTTP • 1: HTTPS • 2: Use HTTPS if SIP transport mode is TLS, otherwise use HTTP.

Table continues…

Parameter name	Default value	Description
CONTACT_NAME_FORMAT	0	Specifies how contact names are displayed. Value operation: • 0: The name format is Last name, First name. • 1: The name format is First name, Last name.
CONTROLLER_SEARCH_INTERVAL	16	Specifies the number of seconds the phone waits to complete the maintenance check for monitored controllers. Valid values are 4 through 3,600.
COUNTRY	USA	Used for network call progress tones. • For Argentina use keyword Argentina. • For Australia use keyword Australia. • For Brazil use keyword Brazil. • For Canada use keyword USA. • For France use keyword France. • For Germany use keyword Germany. • For Italy use keyword Italy. • For Ireland use keyword Ireland. • For Mexico use keyword Mexico. • For Spain use keyword Spain. • For United Kingdom use keyword UK. • For United States use keyword USA. Country names with spaces must be enclosed in double quotes.
D		

Table continues…

Parameter name	Default value	Description
DATEFORMAT	Null	Specifies the format for dates displayed in the phone. The phone screen displays mm or dd in topline and Recents application. yy or yyyy is displayed only on the phone ScreenSaver when Date is enabled. Only / — . separators are supported. • Use %d for day of month • Use %m for month in decimal format. • Use %y for year without century (e.g., 07). • Use %Y for year with century (e.g., 2007). Any character not preceded by % is reproduced exactly. For example, the phone topline to read mm/dd ,and the ScreenSaver to read mm/dd/yy, set %m/%d/%y. Similarly for dd-mm, and dd-mm-YYYY, set %d-%m-%Y
DAYLIGHT_SAVING_SETTING_MODE	2	Specifies daylight savings time setting for phone. Value operation: • 0: Daylight saving time not activated • 1: Daylight saving time is activated. Time set to DSTOFFSET. • 2: Activates automatic daylight savings adjustment as specified by DSTSTART and DSTSTOP.
DELETE_MY_CERT	0	Specifies whether the installed identity certificate, using SCEP or PKCS12 file download, will be deleted. • 0: Installed identity certificate remains valid. • 1: Installed identity certificate is removed.

Table continues…

Parameter name	Default value	Description
DES_STAT	2	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 • 3: to set the devices to automatically use DES without the need to select yes on the prompt.
DHCPSTAT	3	Specifies whether DHCPv4, DHCPv6 or both are used if IPv6 support is enabled by IPV6STAT. **Note:** DHCPv4 is always enabled in IPv4 only and dual mode. DHCPv4 is disabled in IPv6 only mode. Value operation: • 1: run DHCPv4 only. • 2: run DHCPv6 only. • 3: run both DHCPv4 and DHCPv6.
DHCPSTD	0	Specifies whether DHCP complies with the IETF RFC 2131 standard and continues to use the expired DHCP lease. Value operation: • 0: Continue using the address in an extended rebinding state. • 1: Immediately stop using the address.
DIALPLAN	Null	Specifies the dial plan used in the phone. Dialplan accelerates dialing by eliminating the need to wait for the INTER_DIGIT_TIMEOUT timer to expire. The value can contain 0 to 1,023 characters. The default value is null.

Table continues…

Parameter name	Default value	Description
DIALING_MODE_DEFAULT	1	Specifies the dialing mode. If this parameter is set to "Automatic" or "Manual", then it specifies default dialing mode. If this parameter is set to forced, then the option to pick dialing mode disappears from Phone UI user menu.
DIGIT_MAPPING	Null	Specifies a digit map the phone uses to match digits to ensure a complete number is dialed, to transform dialed digits, and block numbers from being dialed. ',' is used for rules separation. Valid value is a string of alphanumeric rules. If a rule uses incorrect characters, the phone ignores it. The preferred way of configuring this parameter is through the web interface.
DIRUSERNAME	Null	Specifies the LDAP client username. The following characters are allowed: • 0–9 • a-z • A-Z The preferred way of configuring this parameter is through the web interface. **Note:** Avaya J129 IP Phone does not support this parameter.
DIRPASSWORD	Null	Specifies the LDAP client password. The following characters are allowed: • 0–9 • a-z • A-Z The preferred way of configuring this parameter is through the web interface. **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
DIRSECURE	1	Specifies whether to use TLS or TCP for the LDAP server. Value operation: • 0: Use TCP • 1: Establish TLS connection using the STARTTLS extended operation. • 2: Establish TLS connection using the Secure LDAP protocol (LDAPS) For example, `SET DIRSECURE 1` There is a difference between STARTTLS and LDAPS: STARTTLS uses the same port as the LDAP protocol. The DIRSRVRPRT parameter value must be the same as the port configured for the LDAP (not for LDAPS) protocol on the server side. The LDAPS protocol uses a port different from LDAP. The value for DIRSRVRPRT needs to correspond to server port for the LDAPS connection. **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
DIRAUTHTYPE	1	Specifies the kind of authentication that is used if the value of the DIRUSERNAME parameter is not null. Value operation: • 0: Simple LDAP authentication. Normally the DIRUSERNAME parameter must contain a DN name of an LDAP record, and DIRUSERNAME must contain a password associated with the record. • 1: Simple LDAP Authentication and Security Layer (SASL). If a connection is established over TLS (DIRSECURE is set to 1 or 2), DIGEST-MD5 or PLAIN authentication mechanisms are supported. If the connection established over TCP (DIRSECURE is set to 0) DIGEST-MD5 is the only supported mechanism. **Note:** Avaya J129 IP Phone does not support this parameter.
DIRENABLED_PLATFORM	0	Determines whether the LDAP directory search is enabled on the phone. Value operation: • 0: No • 1: Yes **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
DIRNAME_FIELDS	cn	Specifies the attributes and their order, shown in the search results. Users can view other attributes, pressing the **Details** soft key. T The attributes, specified in this parameter must be a subset of the attributes, specified in DIRNAME_FIELDS. For example, `SET DIRNAME_FIELDS "cn,sn"` In this example, each match on a search result list displays a last name and a first name. **Note:** Avaya J129 IP Phone does not support this parameter.
DIRNUMBER_FIELDS	telephoneNumber	Specifies the LDAP fields that contain a callable number. The first number listed becomes the primary number. For example, `SET DIRNUMBER_FIELDS "telephoneNumber,mobile,DoD SIP URI"` **Note:** Avaya J129 IP Phone does not support this parameter.
DIRSEARCH_FIELDS	"cn,sn,telephoneNumber"	Specifies LDAP search attributes. The exact number and names of the search attributes depend on the LDAP server configuration and can vary from one LDAP directory to another. When configuring this parameter, you must use attribute names that coincide with the selected LDAP server attribute names. For example, `SET DIRSEARCH_FIELDS "givenName,mail,middle initials, telephoneNumber,sn,mobile ,o ,department ,Rank ,office ,DoD SIP URI"` **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
DIRSECURE	1	Specifies whether to use TLS or TCP for LDAP. To authenticate the server, startTLS is used. ldaps:// is not supported. You need to configure startTLS for the secure LDAP connection. Value operation: • 0: Use TCP • 1: Use TLS For example, `SET DIRSECURE 1` **Note:** Avaya J129 IP Phone does not support this parameter.
DIRSHOW_FIELDS	"cn,sn,telephoneNumber,Mail"	Specifies LDAP detail show fields. The phone returns the attributes, specified in this parameter, for each match found for a search query. You can use this parameter to map the specified LDAP keywords. This mapping defines the way the phone displays show fields. For example, `SET DIRSHOW_FIELDS "dn=Distinguished Name, rank, gn=First Name,office=Office,middle initials=Middle Initial,Display Name=Full Name,sn=Last Name,job title=Job,cn=Common Name,o=Office,c=Country,department=Department,street=Street,mail=Mail Box,l,telephoneNumber=PhoneNumber,st, mobile=Mobile,postalCode=Postal code,facsimileTelephoneNumber=Fax,DoD SIP URI=Number"` In this example, the format is as follows: `SET DIRSHOW_FIELDS "[LDAP Attributes]=[Field Names],[LDAP Attribute 1]=[Field Name1]"` **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description

DIRSRVR	Null	Specifies the IP address or a fully qualified domain name (FQDN) of the LDAP directory server.
		The valid value is an IPv6, IPv4 address in the dotted decimal format or a FQDN.
		For example,
		`SET DIRSRVR 192.168.161.54`
		or
		`SET DIRSRVR domain.com`
		Note:
		Avaya J129 IP Phone does not support this parameter.

DIRSRVRPRT	389	Specifies the port number for the LDAP directory server. Valid values are positive integers from 1 to 65535. For example, `SET DIRSFVFRT 389` **Note:** Avaya J129 IP Phone does not support this parameter.
DIRTOPDN	Null	Specifies the LDAP search base. For example, `SET DIRTOPDN "dc=global,dc=avaya,dc=com"` **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
DIR_TO_LOCAL_MAPPING	"displayName:Name,telephoneNumber:Work,mobile:Mobile"	Specifies mapping of LDAP fields to local contact fields. If there is no rule for at least one contact number, the entire contact mapping is disables. Local contact field names can be assigned from the following: • "firstName" • "nickname" • "URI" • "extension" • "email" • "department" • "zipCode" • "country" for number types: • "work" • "home" • "mobile" • "other" **Note:** Avaya J129 IP Phone does not support this parameter.
DIR_LDAP_DESCRIPTION	“LDAP Directory	Specifies a custom label to be used for the LDAP directory in the Contacts application. Valid value is a text string. **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
DISCOVER_AVAYA_ENVIRONMENT	1	Specifies dynamic feature set discovery. Value operation: • 1: The phone discovers and verifies if the controller supports the AST feature set or not. The phone sends a SUBSCRIBE request to the active controller for the Feature Status Event Package (avaya-cm-feature-status). If the request succeeds, the phone proceeds with PPM Synchronization. If the request is rejected, or is proxied back to the phone, or does not receive a response, the phone assumes that AST features are not available. • 0: The phone operates in a mode where AST features are not available. **Note:** Set the parameter to 0 for an Open SIP environment.
DISPLAY_NAME	Null	Specifies that the display name will be used for the remote party if the server supports a phone providing its own display name. This parameter is used only in 3PCC environment. Parameter values must not include the following symbols: ";<>/&.
DISPLAY_SSL_VERSION	0	Specifies whether OpenSSL and OpenSSH versions are displayed in the **Admin** menu. Value operation: • 0: OpenSSL and OpenSSH versions are not displayed. • 1: OpenSSL and OpenSSH versions are displayed.
DNSSRVR	Null	Specifies a list of DNS server addresses. Valid values are addresses in dotted-decimal (IPv4) or colon-hex (IPv6, if supported) format, separated by commas without spaces.

Table continues…

Parameter name	Default value	Description
DOMAIN	Null	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 can be set through: • DHCP • The settings file. Setting this parameter through the settings file overwrites any values set through DHCP.
DOWNLOADABLE_DIRECTORY	Null	Specifies the file name of the contacts directory. The value can contain 0 to 32 ASCII characters. **Important:** The file name must be in .xml format.
DOT1X	0	Specifies the 802.1X pass-through operating mode. Pass-through is the forwarding of EAPOL frames between the phone Ethernet line interface and its secondary (PC) Ethernet interface Value operation: • 0: EAPOL multicast pass-through enabled without proxy logoff. • 1: EAPOL multicast pass-through enabled with proxy logoff. • 2: EAPOL multicast pass-through disabled.
DOT1XEAPS	MD5	Specifies the authentication method to be used by 802.1X. Valid values are MD5, and TLS.

Table continues…

Parameter name	Default value	Description
DOT1XSTAT	0	Specifies the 802.1X supplicant operating mode. Value operation: 0: Supplicant disabled 1: Supplicant enabled, but responds only to received unicast EAPOL messages 2: Supplicant enabled; responds to received unicast and multicast EAPOL messages
DSCPAUD	46	Specifies the layer 3 Differentiated Services (DiffServ) Code Point for audio frames generated by the phone. Valid values are from 0 to 63. This parameter can also be set through the LLDP, which overwrites any value in the settings file.
DSCPAUD_FL	43	Specifies the DSCP value for flash precedence or priority level voice call. Valid values are from 0 to 63.
DSCPSIG	34	Specifies the layer 3 Differentiated Services (DiffServ) Code Point for signaling frames generated by the phone. Valid values are 0 through 63. This parameter can also be set through LLDP, which overwrites any value set in the settings file.
DSTOFFSET	1	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.
DSTSTART	2SunMar2L	Specifies when to apply the offset for daylight savings time. The date and time for applying the offset can be set in the following formats: • `odddmmmht`: for example, `2SunMar2L` which corresponds to the second Sunday in March at 2 AM local time; • `Dmmmht`: for example, `10Mar5L` which corresponds to March 10 at 5 AM local time.

Table continues…

Parameter name	Default value	Description
DSTSTOP	1SunNov2L	Specifies when to stop applying the offset for daylight savings time. You can set the date and time when the offset is stopped in the following formats: • `odddmmmht`: for example, `1SunNov2L` which corresponds to the first Sunday in November at 2 AM local time; • `Dmmmht`: for example, `7Nov5L` which corresponds to November 7 at 5 AM local time.
DTMF_PAYLOAD_TYPE	120	Specifies the RTP payload type to be used for RFC 2833 signaling. Valid values are 96 through 127.
E		
EASG_SITE_AUTH_FACTOR	Null	Specifies Site Authentication Factor code associated with the EASG site certificate being installed. Valid values are 10 to 20 character alphanumeric string.
EASG_SITE_CERTS	Null	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. The URLs must be separated by commas without any intervening spaces. Valid values are 0 to 255 ASCII characters.
EEESTAT	1	Specifies Energy-Efficient Ethernet (802.3az) is enabled on PHY1 and PHY2. Value operation: • 0: EEE is disabled on both PHY1 and PHY2. • 1: EEE is enabled on both PHY1 and PHY2. This parameter is supported by only Avaya J129 IP Phone.

Table continues…

Parameter name	Default value	Description
EFFECT_OF_REDIAL_BUTTON	1	Specifies whether to show a list or one number on the **Redial** soft key on the phone. Value operation: • 0: Redial out of list. • 1: One number. • 2: option provided by REDIAL_LIST_MODE_DEFAULT parameter on Redial Softkey
ELD_SYSNUM	1	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(default): Enable ELD for System Numbers **Note:** Avaya J139 IP Phone does not support the Busy Indicator feature.
ENABLE_3PCC_ENVIRONMENT	1	Specifies that the phone is working in an Open SIP environment. Value operation: • 0: Disabled • 1: Enabled
ENABLE_AUTO_ANSWER_SUPPORT	0	Specifies that the auto-answer feature is enabled. Value operation: • 0: Disabled • 1: Enabled **Note:** This parameter is only applicable if an Open SIP environment is configured.

Table continues…

Parameter name	Default value	Description
ENABLE_AVAYA_ENVIRONMENT	1	Specifies whether the phone is configured to be used in an Avaya or an Open SIP proxy environment. Value operation: • 0: Configured for a third-party proxy with SIPPING 19 features. • 1: Configured for Avaya with AST features . **Note:** Set the parameter to 0 for an Open SIP environment.
ENABLE_BLIND_TRANSFER	1	Specifies that whether the blind transfer is enabled or not. Value operation: • 0: Disabled. • 1: Enabled. **Note:** Avaya J129 IP Phone does not support this feature.
ENABLE_CALL_LOG	1	Species if call logging and associated menus are available on the phone. Value operation: • 0: No • 1: Yes
ENABLE_CONTACTS	1	Specifies if the contacts application and associated menus are available on the phone. Value operation: • 0: No • 1: Yes
ENABLE_DIGIT_MAPPING	0	Specifies if the phone uses DIGIT_MAPPING parameter for dial plan configuration, if the parameter is disabled DIALPLAN and ELD parameters are used. Value operation: • 0: Disabled • 1: Enabled

Table continues…

Parameter name	Default value	Description
ENABLE_DND	1	Specifies that the do-not-disturb feature is enabled. Value operation: • 0: Disabled • 1: Enabled **Note:** This parameter is only applicable if an Open SIP environment is configured.
ENABLE_DND_PRIORITY_OVER_CFU_CFB	0	Specifies that the Do-not-disturb (DND) feature is given priority over Call forwarding unconditionally (CFU) and Call forwarding busy (CFB). Value operation: • 0: Disabled • 1: Enabled **Note:** This parameter is only applicable if an Open SIP environment is configured.
ENABLE_EARLY_MEDIA	1	Specifies if the phone sets up a voice channel to the called party before the call is answered. Value operation: • 0: No • 1: Yes Setting this parameter to 1 can speed up call setup.
ENABLE_EXCHANGE_REMINDER	0	Specifies whether or not exchange reminders will be displayed. Value operation: • 0: Not displayed • 1: Displayed **Note:** Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description
ENABLE_G711A	1	Specifies if the G.711 a-law codec is enabled. Value operation: • 0: Disabled • 1: Enabled
ENABLE_G711U	1	Specifies ifr the G.711 mu-law codec is enabled. Value operation: • 0: Disabled • 1: Enabled
ENABLE_G722	1	Specifies if the G.722 codec is enabled. Value operation: • 0: Disabled • 1: Enabled
ENABLE_G726	1	Specifies if the G.726 codec is enabled. Value operation: • 0: Disabled • 1: Enabled
ENABLE_G729	1	Specifies if the G.729A codec is enabled. Value operation: • 0: Disabled • 1: Enabled without Annex B support (default). • 2: Enabled with Annex B support.
ENABLE_GDPR_MODE	0	Specifies if Global data Protection Regulations (GDPR) are applied on the phone. If on, it generally ensures that the phones stores unencrypted private data for no longer than 24 hours. Value operation: • 0: GDPR mode is disabled • 1: GDPR mode is enabled Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
ENABLE_HOLD_REMINDER_DISPLAY	1	Specifies whether the called party name or number with the text hc [Return] is displayed on call appearance when the phone reminds the user about a held call. Value operation: • 0: The called party name or number is displayed on call appearance when the phone reminds the user about a held call. • 1: The called party name or number with the text hc [Return] is displayed on call appearance when the phone reminds the user about a held call.
ENABLE_HSTS	0	Specifies whether the phone sends the HTTP Strict Transport Security (HSTS) header in the HTTP response. If you enable this value, the phone sends the header only when the web UI is accessed over the HTTPS. Value operation: • 0: Disabled, the phone does not send the HSTS header in HTTP response. • 1: Enabled, the phone sends the HSTS header in HTTP response.
ENABLE_IPOFFICE	0	Specifies whether the J100 phone can operate in 2 different modes with IP Office. The first mode allows native support of the J100 phone with IP Office with a limited feature set. The second mode allows support of the J100 phone with additional feature support driven by the IP Office proxy. Value operation: • 0: The phone does not support IP Office (except in Avaya Aura failover mode). • 1: The phone supports IP Office in a native environment. • 2: The phone supports IP Office with additional features driven by the IP Office proxy Avaya J129 IP Phone supports value 0 and 1. Avaya J139 IP Phone, Avaya J159 IP Phone and Avaya J169/J179 IP Phone supports value 0 and 2.

Table continues…

Parameter name	Default value	Description
ENABLE_MLPP	0	Specifies that whether the Multiple Level Precedence and Preemption (MLPP) is enabled or not. Value operation: • 0: Disabled. • 1: Enabled.
ENABLE_MODIFY_CONTACTS	1	Specifies if the list of contacts and the function of the contacts application can be modified on the phone. Value operation: • 0: No • 1: Yes
ENABLE_MULTIPLE_CONTACT_WARNING	1	Specifies if a warning message must be displayed if there are multiple phones registered on a user's behalf. Value operation: • 0: No • 1: Yes **Note:** Multiple registered phones can lead to service disruption.
ENABLE_OOD_MSG_TLS_ONLY	1	Specifies if 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. **Note:** A value of 0 is only intended for testing purposes.

Table continues…

Parameter name	Default value	Description
ENABLE_OOD_RESET_NOTIFY	0	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. Value operation: • 0: OOD is not supported. • 1: OOD is supported.
ENABLE_PARK_DYNAMIC_AND_PAGE	0	Specifies whether the Park and Page feature is available to the user. The Park Dynamic and Page feature requires that the CALL_PARK_DYNAMIC_FAC code and CALL_PARK_DYNAMIC_METHOD are defined in order to park the call Value operation: • 0: Park Dynamic and Page feature is not available to the user(Default) • 1: Park Dynamic and Page feature is available to the user. **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
ENABLE_PHONE_LOCK	0	Specifies whether a soft key on the Idle phone screen and a feature button are displayed to allow the user to manually lock the phone. Value operation: • 0: Disabled. **Lock** soft key and feature button are not displayed. • 1: Enabled. **Lock** soft key and feature button are displayed. **Note:** If you enable the parameter, the **Lock** application is available in the **Main menu**. User can use Phone key customization to present the **Lock** application in the main phone screen. There is no **Lock** soft key or feature button. If you disable the parameter, there is no **Lock** application. User does not have the option to present **Lock** application using Phone key customization in the main phone screen.
ENABLE_PUBLIC_CA_CERTS	1	Specifies whether the out-of-the-box phone can validate server certificates against a list of well-known public Certificate Authority certificates Value operation: • 0: Embedded public CA certificates are only trusted when TRUSTCERTS is empty. • 1: Embedded public CA certificates are always trusted.

Table continues…

Parameter name	Default value	Description
ENABLE_RANDOM_RTP_PORT	0	Specifies whether the random RTP port is enabled. Value operation: • 0: Even numbered RTP ports starting at RTP_PORT_LOW will be used for all calls. • 1: Even numbered RTP port will be randomly selected in the range from RTP_PORT_LOW to RTP_PORT_LOW +RTP_PORT_RANGE each time audio path is established. For example: when a call is answered or a call is resumed. To maximize the effectiveness of this setting, RTP_PORT_RANGE should be assigned a value much larger than the default of 40.
ENABLE_RECORDING	0	Specifies if audio debug recording is enabled for users. Value operation: • 0: Audio debug recording is disabled. • 1: Audio debug recording is enabled.
ENABLE_REDIAL	1	Specifies if **Redial** soft key is available. Value operation: • 0: No • 1: Yes
ENABLE_REDIAL_LIST	1	Specifies if the phone redials last number or displays list of recently dialed numbers. Value operation: • 0: Last number redial • 1: Select the last number redial or from the redial list. **Note:** Avaya J129 IP Phone do not support this feature.
ENABLE_RFC5922	1	Specifies to enable or disable the RFC5922 certificate validation. Value operation: • 0: disable validation • 1: enable validation

Table continues…

Parameter name	Default value	Description
ENABLE_SHOW_EMERG_SK	2	Specifies if **Emergency** soft key, with or without a confirmation screen, is displayed when the phone is registered. **Note:** Emergency calls are not supported in an Open SIP environment. Value operation: • 0: **Emergency** soft key is not displayed. • 1: **Emergency** soft key is displayed without a confirmation screen. • 2: **Emergency** soft key is displayed with a confirmation screen.
ENABLE_SHOW_EMERG_SK_UNREG	2	Specifies if an **Emergency** soft key, with or without a confirmation screen, is displayed when the phone is not registered. All emergency numbers will always be supported. Value operation: • 0: **Emergency** soft key is not displayed. • 1: **Emergency** soft key is displayed without a confirmation screen. • 2: **Emergency** soft key is displayed with a confirmation screen.
ENABLE_SIP_USER_ID	0	Specifies the display of the user ID input field on the Login Screen. Value operation: • 0: Disabled • 1: Enabled
ENABLE_SIPURI_HOST_VALIDATION	1	Specifies allowing to accept SIP URI with unrecognized host part in INVITE message. Value operation: • 0: Does not allow • 1: Allows

Table continues…

Parameter name	Default value	Description
ENABLE_STRICT_USER_VALIDATION	0	Specifies that the validation is done for the **To header** and **Request-URI** against AOR and **Contact** header during phone registration. Value operation: • 0: No validation. • 1: Validates the phone registration.
ENABLE_UDP_TRANSPORT	1	Specifies that the UDP option is available on the phone user interface for selection. The UDP option is available along with TCP and TLS. Value operation: • 0: Disabled • 1: Enabled
ENABLE_USBsoHEADSET	1	Specifies whether the USB headset feature is enabled or not. Value operation: • 0: Disabled • 1: enabled
ENABLE_USBKEYBOARD	1	It enables or disables the USB keyboard support. This parameter ignores the other values if the value is set to 1 (enabled by default). Value operation: 0: Disabled 1: Enabled **Note:** This feature is available only on the Avaya J159 IP Phone and Avaya J189 IP Phone.

Table continues…

Parameter name	Default value	Description
ENABLE_USBSTICK	1	It enables or disables the USB stick support. This parameter ignores the other values if the value is set to 1 (enabled by default). Value operation: 0: Disabled 1: Enabled **Note:** This feature is available only on the Avaya J159 IP Phone and Avaya J189 IP Phone.
ENABLE_WEBSERVER	0	Enables or disables the web server to configure the phones in a web browser. Value operation: • 0: Disable • 1: Enable
ENABLE_WMLPUSH_ALERTING	Null	Specifies the behavior of WML browser during incoming call. Value operation: 0 (Default): WML browser disappears when the phone starts ringing and an incoming call appears instead. 1: WML browser still appears when the phone starts ringing and user can answer a call by off-hook from WML browser application. **Note:** This parameter is available in • Avaya J169/J179 IP Phone • Avaya J189 IP Phone
ENCRYPT_SRTCP	0	Specifies whether the encrypted SRTCP is supported. Value operation: • 0: Not supported. • 1: Supported.

Table continues…

Parameter name	Default value	Description
ENFORCE_SIPS_URI	1	Specifies if a SIPS URI must be used for SRTP. Value operation: • 0: Not enforced • 1: Enforced **Note:** For 3PCC environments using TLS signaling, must be set to 0.
ENHDIALSTAT	1	Specifies if the algorithm defined by the parameter is used during certain dialing behaviors. Value operation: • 0: Disables algorithm. • 1: Enables algorithm, but not for Contacts. • 2: Enables algorithm, including Contacts. • 3: Unconditionally apply enhanced dialing rules.
ENTRYNAME	0	Specifies if the calling party name, or the VDN or the skill name must be used in **History** entries. Value operation: • 0: Calling Party Name is used. • 1: VDN or the skill name is used. **Note:** Avaya J129 IP Phone does not support this parameter.
ESCALATE_FAC	Null	Specifies the Feature Access Code to invoke Escalation feature. **Note:** This parameter is available in • Avaya J159 IP Phone • Avaya J169/J179 IP Phone • Avaya J189 IP Phone

Table continues…

Parameter name	Default value	Description
EVENT_NOTIFY_AVAYA_MAX_USERS	20	Specifies the maximum number of users to be included in an event notification message from CM/AST-II . Valid values are 0 through 1,000. This parameter is used only for development and debugging purposes.
EXCHANGE_AUTH_USERNAME_FORMAT	0	Specifies the necessary format of the username for http authentication. Value operation: • 0: Office 2003/Office2016 username format. Username= <ExchangeUserDomain \ExchangeUserAccount> or Username= <ExchangeUserAccount> if <ExchangeUserDomain> is empty. • 1: Office 365 format. Username= <ExchangeUserAccount@ExchangeUserDomain> or Username= <ExchangeUserAccount> if <ExchangeUserDomain> is empty. **Note:** Only Avaya J129 IP Phone supports this feature.

Table continues…

Parameter name	Default value	Description
EXCHANGE_AUTH_METHOD_DEFAULT	0	Specifies the Exchange authentication method configured by administrator. When you configure Basic (Forced) or OAuth (Forced) method, it is the active authentication method. The phone user is not allowed to change the authentication method from phone user interface. When you configure non-forced method, phone user can change the authentication method from the phone user interface and configure the active authentication method. Value operation: • **0**: Basic authentication (Default) • **1**: OAuth authentication • **2**: Basic authentication- forced • **3**: OAuth authentication- forced **Note:** Avaya J129 IP Phone does not support this feature.
EXCHANGE_EMAIL_DOMAIN	Null	Specifies the Exchange email domain. The value can contain 0 to 255 characters. **Note:** Only Avaya J129 IP Phone supports this feature.
EXCHANGE_SERVER_LIST	outlook.office365.com	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.

Table continues…

Parameter name	Default value	Description
EXCHANGE_SERVER_SECURE_MODE	1	Specifies if HTTPS should be used to contact Exchange servers. Value operation: • 0: Use HTTP • 1: Use HTTPS **Note:** Avaya J129 IP Phone does not support this feature.
EXCHANGE_SNOOZE_TIME	5	Specifies the number of minutes in which a reminder must be displayed again after it is temporarily dismissed. Valid values are 0 through 60. **Note:** Avaya J129 IP Phone does not support this feature.
EXCHANGE_USER_ACCOUNT_DEFAULT	Null	Specifies the Exchange user account configured by administrator. This parameter is only applicable when authentication method is OAuth. If phone user hasn't configured any user name on the phone user interface then value configured in this parameter would be used. The valid value is a string of up to 255 characters. The default value is empty. **Note:** Avaya J129 IP Phone does not support this feature.
EXCHANGE_USER_DOMAIN	Null	Specifies the domain for the URL used to obtain Exchange contacts and calendar data. The value can contain 0 to 255 characters. **Note:** Only Avaya J129 IP Phone supports this feature.
F		

Table continues…

Parameter name	Default value	Description
FAILED_SESSION_REMOVAL_TIMER	30	Specifies the number of seconds the phone displays a session line appearance and generates re-order tone after an invalid extension is dialed and user does not press the **End Call** soft key. Valid values are 5 through 999. The default value is 30.
FAST_RESPONSE_TIMEOUT	4	Specifies the number of seconds the phone waits before terminating an INVITE transaction if no response is received. Valid values are 0 through 32. Value of 0 means that this timer is disabled.
FIPS_ENABLED	0	Specifies whether the usage of FIPS-140 approved cryptography is enabled or not. Value operation: • 0: (Default). Disables FIPS-140 approved cryptographic algorithms. • 1: Enables only FIPS-140 approved cryptographic algorithms.
FORCE_SIP_EXTENSION	Null	Specifies whether the phone prompts to enter the User ID after the phone powers up.
FORCE_SIP_PASSWORD	Null	Specifies whether the phone prompts to enter the password after the phone powers up.
FORCE_SIP_USERNAME	Null	Specifies whether the phone prompts to enter the username after the phone powers up. This parameter enables the user to force login to the phone during the staging process, prior to the phone's deployment
FORCE_WEB_ADMIN_PASSWORD	Null	Specifies the password to access the phone through Web as Administrator. Valid values are 8 to 31 alphanumeric characters.
FORCE_XSI_USER_ID	Null	Specifies the BroadSoft user ID which the phone must use for XSI authentication. BroadSoft user Id is the SIP user Id excluding at (@) and domain. Valid values are 0 to 255 ASCII characters.

Table continues…

Parameter name	Default value	Description
FORCE_XSI_WEB_PASSWORD	Null	Specifies the BroadSoft's web portal password which the phone must use for XSI web authentication. If the value is null, then SIP authentication method is used.
FQDN_IP_MAP	Null	Specifies a comma separated list of name or 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. String length is up to 255 characters without any intervening spaces inside the string. The purpose of this parameter is to support cases where the server certificate Subject Common Name of Subject Alternative Names includes FQDN, instead of IP address, and the SIP_CONTROLLER_LIST is defined using IP address. This parameter is supported with phone service running over TLS, however, the main use case is for Avaya Aura SM/PPM services. This parameter must not to be used as an alternative to a DNS lookup or reverse DNS lookup.
G		
G726_PAYLOAD_TYPE	110	Specifies the RTP payload type to be used for the G.726 codec. Valid values are 96 through 127.
GMTOFFSET	0:00	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).
————————————

Parameter name	Default value	Description
GUESTDURATION	2	Specifies the duration (in hours) before a Guest Login or a visiting user login is automatically logged off if the phone is idle. Valid values are integers from 1 to 12. **Note:** This parameter is supported by J159 and J169/179 phones.
GUESTLOGINSTAT	0	Specifies whether the Guest Login feature is available to users. Value operation: • 0: The feature is not available. • 1: The feature is available. **Note:** This parameter is supported by J159 and J169/179 phones.
GUESTWARNING	5	Specifies the number of minutes, before time specified by GUESTDURATION, that a warning of the automatic logoff is initially presented to the Guest or Visiting User. Valid values are integers from 1 to 15.
H		
HANDSET_PROFILE_DEFAULT	1	Specifies the number of the default handset audio profile. Valid values are 1 through 20.
HANDSET_PROFILE_NAMES	Null	Specifies an ordered list of names to be displayed for handset audio profile selection. The list can contain 0 to 255 UTF-8 characters. 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 might contain spaces, but if any do, the entire list must be quoted. There is no way to prevent a profile from being displayed.

Table continues…

Parameter name	Default value	Description
HEADSET_PROFILE_DEFAULT	1	Specifies the number of the default headset audio profile. Valid values are 1 through 20. **Note:** Avaya J129 IP Phone does not support this feature.
HEADSET_PROFILE_NAMES	Null	Specifies an ordered list of names to be displayed for headset audio profile selection. The list can contain 0 to 255 UTF-8 characters. Names are separated by commas without any intervening spaces. Two commas in succession indicate a null name, which means that the default name is displayed for the corresponding profile. Names can contain spaces, but if any do, the entire list must be quoted. There is no way to prevent a profile from being displayed. **Note:** Avaya J129 IP Phone does not support this feature.
HEADSYS	0	Specifies whether the phone goes on-hook, if the headset is active when the disconnect message is received. Value operation: • 0: The phone goes on-hook if the disconnect message is received when the headset is active. • 1: Disconnect messages are ignored when the headset is active. • 2: Has the same impact as a value of 0. • 3: Has the same impact as a value of 1.

Table continues…

Parameter name	Default value	Description
HOLD_REMINDER_TIMER	0	Specifies that a reminder (in seconds ranging from 0 to 999) is triggered for a call-on-hold in the following ways: • Audible alert (One ring). • Visual alert (Beacon LED blinks for five seconds). • Appends the text “hc [Return]” at the end of the name or number of the call-on-hold in the line appearance.
HOMEIDLETIME	10 for Avaya J129 IP Phone 10 for other models	Specifies the number of minutes of idle time after which the **Home** screen is displayed. Valid values are 0 through 30. A value of 0 means that the **Home** screen is not displayed automatically when the phone is idle. **Note:** Only Avaya J129 IP Phone supports this feature.
HOTLINE	Null	Specifies zero or one hotline number. Valid values can contain up to 30 dialable characters ranging from 0 to 9, *, and #.
HTTPEXCEPTIONDOMAINS	Null	Specifies a list of one or more domains, separated by commas without any intervening spaces, for which HTTPPROXY is not used. The value can contain 0 to 255 characters. The default value is null.
HTTPDIR	Null	Specifies the path to the configurations and data files in HTTP and HTTPS GET operations during device bootup. This path is relative to the root of the HTTPS file server, to the directory in which the device configuration and date files are stored. If $MACADDR and/or $MODEL4 and/or $SERIALNO macro is present in the configured path then such macro is replaced with its actual value. The value can contain 0 to 127 ASCII characters without space.

Table continues…

Parameter name	Default value	Description
HTTPPORT	80	Sets the TCP port used for HTTP file downloads from non-Avaya servers. Values range from 0 to 65,535.
HTTPPROXY	Null	Specifies the address of the HTTP proxy server used by SIP phones to access an SCEP server that is not on the enterprise network. Valid value can contain 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.
HTTPSRVR	Null	Specifies zero or more HTTP server IP addresses to download configuration script files. The addresses must be separated by commas without any intervening spaces. The format of specifying IP addresses are: • Dotted decimal • Colon-hex • DNS name The parameter can be set by using LLDP. Valid values contains 0 to 255 ASCII characters.
I		
ICMPDU	1	Specifies if ICMP Destination Unreachable messages are generated. Value operation: • 0: No messages are generated. • 1: Limited port unreachable messages are generated. • 2: Protocol and port unreachable messages are generated.
ICMPRED	0	Specifies if received ICMP Redirect messages are processed. Value operation: • 0: No • 1: Yes

Table continues…

Parameter name	Default value	Description
IGNORE_BLF_LINE_KEY	0	Specifies if Softkey1 action will not be performed when user presses line key associated with the BLF line. This parameter is not applicable when user presses BLF key in a conference, transfer, page target or similar selection mode. Value operation: • 0: Softkey1 action is performed • 1: Soktkey1 action is not performed **Note:** Avaya J129 IP Phone does not support this feature.
IGNORE_LINE_KEY	0	Specifies if the action of Softkey1 on the phone screen is performed or ignored when the user's call appearance is on an active call and the user presses the line key associated with the active call. Value operation: • 0: No • 1: Yes **Note:** Avaya J129 IP Phone does not support this feature.
IGNORE_CONTACT_HEADER_DISPLAY_NAME	0	Specifies if the phone is allowed to use a display name from the Contact header when there is no display name in the PAI or From headers. In OpenSIP environment it is recommended to set this parameter to 1. Value Operation: • 0: A display name in the Contact header is permitted to be used (default). • 1: A display name in the Contact header is always ignored.
INGRESS_DTMF_VOL_LEVEL	-12dBm	Specifies the power level of tone, expressed in dBm0. Values can range from -20dBm to -7dBm.

Table continues…

Parameter name	Default value	Description
INTER_DIGIT_TIMEOUT	5	Specifies the number of seconds that the phone waits after a digit is dialed before sending a SIP INVITE. Valid values are 1 through 10.
IPV6DADXMITS	1	Specifies whether Duplicate Address Detection is performed on tentative addresses, as specified in RFC 4862. Value operation: • 0: DAD is disabled • 1 to 5: Maximum number of transmitted Neighbor Solicitation messages.
IPV6STAT	0	Specifies whether IPv6 will be supported or not. Value operation: • 0: IPv6 will not be supported. • 1: IPv6 will be supported.
K		
KEEP_CURRENT_CA	1	Specifies whether the currently active line on the phone screen is still highlighted after the call on the selected line is ended. Valid values: • 0 - Disable. When a call on the selected line is ended, the selection is moved from the current Call Appearance to session line with a higher priority or to the first available line if the phone becomes idle. • 1 - Enable (default). When a call on the selected line is ended, the highlighted line is not changed.
KEYUSAGE_REQUIRED	0	Specifies whether the server certificate is checked for the presence of a Key Usage extension. When enabled, a server certificate is rejected if the Key Usage extension is missing. Value operation: • 0: Key Usage checking is disabled • 1: Key Usage checking is enabled
L		

Table continues…

Parameter name	Default value	Description
L2Q	0	Specifies if layer 2 frames generated by the telephone have IEEE 802.1Q VLAN tags. Value operation: • 0: Auto - VLAN tagging is turned on when the network can support VLAN tagging and L2QVLAN is non zero. • 1: On - VLAN tagging is turned on when the network can support VLAN tagging. The IP phone sends tagged frames with VLAN = L2QVLAN, even if L2QVLAN is set to 0. • 2: Off - VLAN functionality is disabled. **Note:** This parameter can also be set through: • Local admin procedure • A name equal to value pair in DHCPACK message • SET command in a settings file • DHCP option 43 • LLDP
L2QAUD	6	Specifies the layer 2 priority value for audio frames generated by the telephone. Valid values are 0 through 7. **Note:** This parameter can also be set through: • SET command in a settings file • LLDP. Setting this parameter though LLDP overwrites any values in the settings file.

Table continues…

Parameter name	Default value	Description
L2QSIG	6	Specifies the layer 2 priority value for signaling frames generated by the phone. Valid values are 0 through 7. **Note:** This parameter can also be set through: • SET command in a settings file • LLDP • AADS Setting this parameter through LLDP or AADS overwrites values in the settings file.
L2QVLAN	0	Specifies the voice VLAN ID to be used by IP phones. Valid values are 0 through 4,094. **Note:** This parameter can also be set through: • Local admin procedure • A name equal to value pair in DHCPACK message • SET command in the settings file • DHCP option 43 • LLDP
LANGUAGES	Null	Specifies the language files that must installed or downloaded to the phone. Filenames can be full URL, relative pathname, or filename comma separated filenames ending with `.xml`.
LLDP_ENABLED	2	Specifies whether LLDP is enabled. Value operation: • 0: Disabled • 1: Enabled • 2: Enabled, but only begins transmitting if an LLDP frame is received.

Table continues…

Parameter name	Default value	Description
LOCAL_DIAL_AREA_CODE	0	Specifies if user must dial area code for calls within same area code regions. Value operation: • 0: User don't need to dial area code. • 1: User need to dial area code. When enabled, the area code parameter (PHNLAC) should also be configured. **Note:** This parameter is supported when the phone is failed over.
LOCAL_LOG_LEVEL	3	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 are logged. 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:** Setting the value to 7 can impact the performance of the phone because of the number of events generated.

Table continues…

Parameter name	Default value	Description
LOG_CATEGORY	Null	Specifies a list of categories of events to be logged through syslog and locally. This parameter must be specified to log events below the Error level. The list can contain up to 255 characters. Category names are separated by commas without any intervening spaces. H1xx SIP R1.0 and later; the default is ALL which implies all categories. New categories for H1xx compare to 96x1 SIP include ANDROID and KERNEL.
LOG_DIALED_DIGITS	1	Specifies if the call log will contain digits dialed by a user or information about a remote party when the user dials 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).
LOGSRVR	Null	Specifies one address for a syslog server in dotted-decimal format (IPv4), colon-hex format (IPv6, if supported), or DNS name format. The value can contain 0 to 255 characters.
LOGSRVR_SECURE	0	Specifies if the phone uses secure or non-secure syslog transport mode by default. Value operation: • 0: Non-secure mode using UDP transport • 1: Secure mode using TLS transport RFC 5425 Selected value is available as Default option in Administrator menu
M		

Table continues…

Parameter name	Default value	Description
MATCHTYPE	0	Specifies how an incoming or outgoing phone number is compared with the contacts on the phone to display the contact name. 0: Displays the contact name if all the digits match. 1: Displays the contact name if all the digits of the shorter number match with the right-most digits of the longer number. For example, a 5-digit extension number can be matched with the 8-digit phone number saved in the contacts. 2: Displays the contact name if at least the last four digits match. If the contacts are saved in multiple sources, for example, Exchange, or locally, the contact name saved first is displayed.
MAX_TRUSTCERTS	10	Specifies the maximum number of trusted certificates defined by the TRUSTCERTS parameter that can be downloaded to the phone. Each trusted certificate file may contain more than one certificate. MAX_TRUSTCERTS enforces the number of certificates. Valid values are from 1 to 10.
MAX_DNS_DISCOVERED_SIP_CONTROLLERS	2	This parameter specifies the maximum number of the SIP controllers to be used for redundancy from DNS lookup. The value ranges from 2–6 SIP controllers.

Table continues…

Parameter name	Default value	Description
MEDIA_ADDR_MODE	4	Specifies the preference of SDP media group lines [per RFC 4091, 4092 and 5888] and the SDP answer / offer format. **Note:** IPv4 only or IPv6 only phones ignores MEDIA_ADDR_MODE. Value operation, SDP offer in Avaya and Non Avaya environment: • 4: IPv4 (Note 3) • 6: IPv6 (Note 3) • 46: Prefer IPv4 over IPv6 • 64: Prefer IPv6 over IPv4 Value operation, SDP answer in Avaya environment: • 4: IPv4 (Note 1 and 3) • 6: IPv6 (Note 1 and 3) • 46: Follow the remote preference • 64: Follow the remote preference Value operation, SDP answer in Non Avaya environment: • 4: IPv4 (Note 1 and 3) • 6: IPv6 (Note 1 and 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 IPv4 (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 answers 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), answers reject the call with 488, if MEDIA_ADDR_MODE does not match any of offered audio lines (with non-zero port).

Table continues…

Parameter name	Default value	Description
		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. Example : Setting to use IPv6 only SET MEDIA_ADDR_MODE 6 Example : Setting to preference of IPv6 over IPv4 SET MEDIA_ADDR_MODE 64
MEDIA_NEG_PREFERENCE	0	Specifies the address family preference used by a dual mode answer in non-Avaya environment. This parameter is not applicable for single mode phones. Value operation: • 0: Remote or offerer's preference • 1: Local
MEDIA_PRESERVATION	1	Supports media preservation when ENABLE_IPOFFICE is set to 2. Value operation: • 0: Phone tries to preserve a call for a duration specified by PRESERVED_CALL_DURATION settings parameter. • 1: Phone does not preserve a call. As soon as the phone detects link failure to IP Office, the phone drops a call and makes re-registration attempt.

Table continues…

Parameter name	Default value	Description
MEDIAENCRYPTION	9	Specifies which media encryption (SRTP) options are supported. 3 options can be specified in a comma-separated list. The options are: • 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 The list of media encryption options are ordered from high (left) to low (right) options. The phone publishes this list in the SDP-OFFER or chooses from SDP-OFFER list according to the list order defined in MEDIAENCRYPTION.
MP_ENABLED	0	Specifies if the Multicast Paging feature is enabled on the phone. This is the basic parameter for this feature. If this parameter is not set, other parameters listed below will be ignored. Valid values: • 0: Multicast Paging is disabled. • 1: Multicast Paging is enabled.

Table continues…

Parameter name	Default value	Description

MP_GROUPS_TO_LISTEN	Null	Defines the list of Multicast Paging groups that the phone listens to. A maximum of 10 paging groups can be listed.
		The paging groups should be separated with a comma (“,”), and should be listed in the following format:
		`IP:port:priority:label`
		where
		• `IP` is the multicast IP address of an MP group;
		• `Port` is the IP port of a Multicast Paging group, the valid value is an even integer ranging from 1024 to 65534;
		• `Priority` is the priority of a group. Allowed values are 1 through 16, with smaller values indicating a higher priority;
		• `Label` is a group label which is displayed in notification messages when the incoming page from this group is played.
		All the above-listed settings are required.
		For example,
		`SET MP_GROUPS_TO_LISTEN “239.0.0.0:1208:1:Security,239.1.2.3:1210:4:Sales”`

MP_GROUPS_TO_SEND	Null	Defines the list of Multicast Paging groups which the phone can send pages to. Priority is not set for these groups. A maximum of 10 paging groups can be listed.
		The paging groups should be separated with a comma (“,”), and should be listed in the following format:
		`IP:port:label`
		`IP`, `Port`, and `Label` denote the same as the corresponding MP_GROUPS_TO_LISTEN values. All these settings are required.
		For example,
		`SET MP_GROUPS_TO_SEND “239.0.0.0:1208:Sales,239.1.2.3:1210:Team”`

Table continues…

Parameter name	Default value	Description
MP_CODEC	1	Specifies a codec which will be used to code and decode Multicast Paging transmissions. Valid values: • 1: G.729 codec is used. • 2: G.711u codec is used. • 3: G.711a codec is used.
MP_PACKET_SIZE	20	Specifies the size of an RTP packet in milliseconds. The valid values are 10 through 80. The value must be valid for the selected codec and therefore must not be changed unless necessary.
MTU_SIZE	1500	Specifies the maximum transmission unit (MTU) size transmitted by the phone. Valid values are 1496 or 1500. Use 1496 for older Ethernet switches.
MUTE_ON_REMOTE_OFF_HOOK	1	Controls the speakerphone muting for a remote-initiated (a shared control or OOD-REFER) speakerphone off-hook. Value operation: 0: the speakerphone is unmuted 1: the speakerphone is muted **Note:** This parameter is set to 0 in IP Office environment.
MYCERTCAID	CAIdentifier	Specifies an identifier for the CA certificate with which the SCEP certificate request is to be signed, if the server hosts multiple Certificate Authorities. The value can contain zero to 255 ASCII characters.

Table continues…

Parameter name	Default value	Description
MYCERTCN	$SERIALNO	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 phone's serial number) or $MACADDR (which will be replaced by the phone's MAC address), but it can contain other characters as well, including spaces. The value can contain eight ($MACADDR) to 255 characters.
MYCERTDN	Null	Specifies the part the SUBJECT of an SCEP certificate request that is common for all phones. The value must begin with a / and can include Organizational Unit, Organization, Location, State and Country. The value can contain Zero to 255 ASCII characters. **Note:** / must be used as a separator between components. Commas do not work with some servers.
MYCERTKEYLEN	2048	Specifies the bit length of the public and private keys generated for the SCEP certificate request. The value is a 4 ASCII numeric digits. The minimum value is 2048.
MYCERTRENEW	90	Specifies the percentage of the identity certificate's validity interval after which renewal procedure is initiated. Valid values are 1 through 99.
MYCERTURL	Null	Specifies the URL of the SCEP server for obtaining an identity certificate. If the URL is specified in HTTPS, then the HTTPS is used to send the CSR to the SCEP server. The valid values can range from Zero to 255 ASCII characters. The default value is null.
N		

Table continues…

Parameter name	Default value	Description
NAT_SIGNALING_KEEPALIVE_ENABLED	1	Determines whether the telephone sends keep-alives to refresh NAT bindings for the phone's private signaling IP address and port. Valid values: • 0: Keep-alive messages are not sent. • 1: Keep-alive messages are sent.
NAT_SIGNALING_KEEPALIVE_OVERRIDE_SEC	29	Sets the interval, in seconds, between keep-alives used to refresh NAT bindings for the phone signaling IP address and port. Valid values: • None: The phone will use the default value. • 15 – 900: The phone will use this value as the keep-alive interval for every SIP registration and dialog.
NO_DIGITS_TIMEOUT	20	Specifies the number of seconds the phone waits for a digit to be dialed after going off-hook and before generating a warning tone. Valid values are 1 through 60.
O		
OCSP_ACCEPT_UNK	1	Specifies that whether to close a TLS connection during an unknown certificate revocation status. Value operation: • 0: Certificates are revoked and the TLS connection is closed. • 1: Certificates are accepted.
OCSP_CACHE_EXPIRY	2880	Specifies the time interval for the OCSP cache expiry in minutes. Valid range is from 60 to 10,080.
OCSP_ENABLED	0	Specifies that OCSP is used to check the revocation status of the certificates. Value operation: • 0: Disabled. • 1: Enabled for all peer TLS connections on SIP, HTTPS, and EAP-TLS.

Table continues…

Parameter name	Default value	Description
OCSP_HASH_ALGORITHM	0	Specifies the hashing algorithm for OCSP request. Value operation: • 0: SHA1 • 1: SHA256
OCSP_NONCE	1	Specifies that whether a nonce is added in the OCSP requests and expected in the OCSP responses. Value operation: • 0: Not added. • 1: Added.
OCSP_TRUSTCERTS	Null	Specifies the list of OCSP trusted certificates that are used as OCSP signing authority for checking the revocation status of the certificate. This applies to when the OCSP responder is using a different CA.
OCSP_URI	Null	Specifies the URI of an OCSP responder. The URI can be an IP address or hostname. Valid values contain 0 to 255 ASCII characters, zero or one URI.
OCSP_URI_PREF	1	Specifies the preferred URI for use in an OCSP request when more than one source is available. Value operation: • 1: Checks the OCSP_URI and then the OCSP field of the Authority Information Access (AIA) extension of the certificate. • 2: Checks the OCSP field of the Authority Information Access (AIA) extension of the certificate and then the OCSP_URI.
OCSP_USE_CACHE	1	Specifies that the OCSP caching is in use. Value operation: • 0: Checks the OCSP responder and disables the use of OCSP caching. • 1: Enables the use of OCSP caching.
OFF_HOOK_ALERT_TIMER	10	Specifies the length of the alert timer in seconds Value operation: • 1-60: timer in seconds

Table continues…

Parameter name	Default value	Description
OFF_HOOK_ALERT_EXTENSION	Null	Specifies if the off-hook alert feature is enabled and the off-hook alert extension. Value operation: • "": Disabled • An extension number: The phone dials this number in case of an off-hook alert event.
OUTBOUND_SUBSCRIPTION_REQUEST_DURATION	86,400	Specifies the duration in seconds requested by the phone in SUBSCRIBE messages, which can be decreased depending on the response from the server. Valid values are 60 through 31,536,000 (one year). For NetSapiens, the valid value range is 300 through 31,536,000. The default value is equivalent to one day.
OVERRIDE_SOFTKEY_IDLE	0	Specifies if the phone shows default softkeys for CA lines in an IDLE state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_ACTIVE	0	Specifies if the phone shows default softkeys for CA lines in an ACTIVE state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_HELD		Specifies if the phone shows default soft keys for CA lines in an HELD state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_INCOMING	0	Specifies if the phone shows default softkeys for CA lines in an INCOMING state. Value operation: • 0: No • 1: Yes

Table continues…

Parameter name	Default value	Description
OVERRIDE_SOFTKEY_INCOMING_VISUAL	0	Specifies if the phone shows default softkeys for CA lines in an INCOMING_VISUAL state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_OUTGOING	0	Specifies if the phone shows default softkeys for CA lines in an OUTGOING state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_ACTIVE_PAGETARGET	0	Specifies if the phone shows default softkeys for CA lines in ACTIVE_PAGE state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_BLF_ACTIVE	0	Specifies if the phone shows default softkeys for BLF lines in ACTIVE state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_BLF_IDLE	0	Specifies if the phone shows default softkeys for BLF lines in IDLE state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_BLF_INCOMING	0	Specifies if the phone shows default softkeys for BLF lines in ALERTING state. Value operation: • 0: No • 1: Yes

Table continues…

Parameter name	Default value	Description
OVERRIDE_SOFTKEY_BLF_INCOMING_VISUAL	0	Specifies if the phone shows default softkeys for BLF lines in ALERTING state on the incoming call view. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_BLF_OUTGOING	0	Specifies if the phone shows default softkeys for BLF lines in OUTGOING_RING state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_IDLE	0	Specifies if the phone shows default soft keys for shared lines in an IDLE state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_ACTIVE	0	Specifies if the phone shows default soft keys for shared lines in an ACTIVE state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_INCOMING	0	Specifies if the phone shows default soft keys for shared lines in an INCOMING state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_INCOMING_VISUAL	0	Specifies if the phone shows default soft keys for shared lines in an INCOMING_VISUAL state. Value operation: • 0: No • 1: Yes

Table continues…

Parameter name	Default value	Description
OVERRIDE_SOFTKEY_SCA_OUTGOING	0	Specifies if the phone shows default soft keys for shared lines in an OUTGOING state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_HELD	0	Specifies if the phone shows default soft keys for shared lines in an HELD state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_ACTIVE_PAGETARGET	0	Specifies if the phone shows default soft keys for shared lines in an ACTIVE_PAGE state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_CONFERENCE_DIALING	0	Specifies if the phone shows default softkeys for shared lines in an Transfer Dialing state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_CONFERENCE_OUTGOING	0	Specifies if the phone shows default softkeys for shared lines in an Conference Outgoing state. Value operation: • 0: No • 1: Yes
OVERRIDE_SOFTKEY_SCA_CONFERENCE_CONSULT	0	Specifies if the phone shows default softkeys for shared lines in an Conference Consult state. Value operation: • 0: No • 1: Yes

Table continues…

Parameter name	Default value	Description
OVERRIDE_SOFTKEY_SCA_CONFERENCE_ACTIVE	0	Specifies if the phone shows default softkeys for shared lines in an Conference Consult state. Value operation: • 0: No • 1: Yes
P		
PHNCC	1	Specifies the country code for United States. The value is 1. Valid values 1 to 999.
PHNDAC	Null	Dial access code - will be applied if the dialed number length + the length of the Dial access code length equals the national number length. This calculation does not include an outside line access code. It is different from PHNLAC since PHNLAC is applied when the phone number length is more than ext number length and less than national number length.
PHNDPLENGTH	5	Specifies the internal extension number length. If your extension is 12345, and your dial plan length is 5. The maximum extension length is 13. This value must match the extension length set on your call server. Valid values are 3 through 13.
PHNEMERGNUM	Null	Specifies an emergency phone number to be dialed if the associated button is selected. Valid values can contain up to 30 dialable characters (0-9, *, #).
PHNIC	011	Specifies the international access code. For the United States, the value is 011. Valid values are 0 to 4 dialable characters (0-9,*,#).

Table continues…

Parameter name	Default value	Description
PHNLAC	Null	Phone's Local Area Code indicates the phone's local area code, which along with the parameter LOCAL_DIAL_AREA_CODE, allows users to dial local numbers with more flexibility. PHNLAC is a string representing the local area code the phone. **Note:** This parameter is supported when the phone is failed over.
PHNLD	1	Specifies the long distance access code. Valid values are 0 through 9 and empty string. If long distance access code is not needed then set the parameter to null.
PHNLDLENGTH	10	Specifies the national phone number length. For example, 800-555-1111 has a length of 10. Valid values are 5-15.
PHNMOREEMERGNUMS	Null	Specifies list of comma separated emergency numbers. Valid values can contain up to 30 dialable characters (0-9, *, #).
PHNMUTEALERT_BLOCK	1	Specifies if the **Mute Alert** feature is blocked or unblocked. Value operation: • 0: Unblocked • 1: Blocked
PHNNUMOFSA	3	Specifies the number of session appearances the phone must support while operating in an non-Avaya environment. Valid values are 1 through 10.
PHNOL	9	Specifies the outside line access code. This is the number you press to make an outside call. Valid values are 0 to 2 dialable characters (0 - 9, *, #).

Table continues…

Parameter name	Default value	Description
PHONEKEY	Null	Specifies the list of pre-configured keys. For the PHONEKEY syntax rules and values, refer to Pre-configuration of keys parameter on page 221 and PHONEKEY parameter values on page 552.
PHONE_LOCK_IDLETIME	0	Specifies the interval of idle time, in minutes, after which the phone will automatically lock. Value operation: • 0: Phone will not lock automatically. Valid values are 0 through 10,080.
PHONE_LOCK_PASSWORD_FAILED_ATTEMPTS	8	Specifies the number of consecutive failed attempts that you permit to unlock the phone. After the maximum is reached, the user will be blocked from further attempts for a period of time before being allowed to attempt again. If you set the value to 0, the user will never be blocked from attempting to unlock the phone.
PHONE_LOCK_PASSWORD_LOCKED_TIME	5	Specifies the length of time that you set where the user will be blocked from attempting to unlock the phone if the user exceeds the maximum number of failed unlock attempts. The value ranges between 5–1440 minutes.
PHONE_LOCK_PIN	Null	Specifies the PIN that you set for the user to enter it to unlock the phone. The value can be only digits, ranging between 4–20 characters. if you do not set any value here, the SIP password can be used for unlocking the phone.

Table continues…

Parameter name	Default value	Description
PHONE_SCREEN_MODE	1	Specifies the screen mode used on the phone by default and whether the user can change this setting in the Settings menu. Valid values: • 0: Non-forced Half Screen mode is used by default, and the Display menu is available on the phone. The user can change the screen width setting manually to override the PHONE_SCREEN_MODE parameter value. • 1: Non-forced Full Screen mode is set. This is a default value which is used at the first boot-up of the phone. The Display menu is available under the Settings menu, and the user can change the screen width setting manually to override the PHONE_SCREEN_MODE parameter value. If PHONE_SCREEN_MODE is set to 1 after the phone screen mode is set to Half, this setting will have no effect. • 2: Forced Half Screen mode is used on the phone, and this setting cannot be changed by the user. • 3: Forced Full Screen mode is used on the phone, and this setting cannot be changed by the user. **Note:** Avaya J129 IP Phone does not support this feature.
PHY1STAT	1	Specifies the speed and duplex settings for the Ethernet line interface. 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-negotiated

Table continues…

Parameter name	Default value	Description
PHY2_AUTOMDIX_ENABLED	1	Specifies whether auto-MDIX is enabled on PHY2. Value operation: • 0: auto-MDIX is disabled. • 1: auto-MDIX is enabled.
PHY2PRIO	0	Specifies the layer 2 priority value to be used for frames received on the secondary Ethernet interface when VLAN separation is enabled. Valid values are 0 through 7. **Note:** J129 does not support this parameter.
PHY2STAT	1	Specifies the speed and duplex settings for the secondary (PC) Ethernet interface. 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-negotiated
PHY2TAGS	0	Determines whether or not VLAN tags are stripped on Ethernet frames going out of the Computer (PC) port. Value operation: • 0: Strip tags. VLAN tags are stripped from Ethernet frames leaving the computer (PC) port of the phone. • 1: Does not strip tags. VLAN tags are not stripped from Ethernet frames leaving the Computer (PC) port of the phone. **Note:** This parameter is configured through the settings file.

Table continues…

Parameter name	Default value	Description
PHY2VLAN	0	Specifies the value of the 802.1Q VLAN ID used by frames forwarded to and from the secondary (PHY2) Ethernet interface when VLAN separation is enabled. Valid values are 0 through 4094. **Note:** The parameter is configured through the following: • SET command in a settings file • LLDP
PKCS12_PASSWD_RETRY	3	Specifies the number of retries for entering PKCS12 file password. 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. Valid values are from 0 to 100. Value operation: • 0: No retry
PKCS12URL	Null	Specifies the URL to be used to download a PKCS #12 file containing an identity certificate and its private key. Valid values contain 0 to 255 ASCII characters, zero or one URL. The value can be a string that contains either $SERIALNO or $MACADDR, but it may contain other characters as well. If $MACADDR is added to the URL, then the PKCS12 filename on the file server includes MAC address without colons. PKCS12 file download is preferred over SCEP if PKCS12URL is defined. Value operation: • Null: (Default) Specifies that the PKCS#12 identity certificate download is disabled. • 0 – 255 characters.

Table continues…

Parameter name	Default value	Description
PLAY_TONE_UNTIL_RTP	1	Specifies whether locally-generated ringback tone stops 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).
PRESERVE_MEDIA_CONNECTIONS	0	Specifies whether to preserver media connections for the servers that do not comply with RFC 3264 8.2. Value operation: • 0: Do not preserve media connections. • 1: Preserver media connections.
PRESERVED_CALL_DURATION	120	Specifies the time interval in minutes if ENABLE_IPOFFICE is set to 2 and if MEDIA_PRESERVATION is set to 1. The time interval can be from 10 minutes to 120 minutes.
PRIMARY_LINE_EXTENSION	Null	Specifies the default label for primary shared and private lines. This value is used if the label for a primary call appearance is not customized. **Note:** This value is optional. If not provided FORCE_SIP_USERNAME value is used.

Table continues…

Parameter name	Default value	Description
PRIMARY_LINE_BARGE_IN_ENABLED	1	Specifies whether the **Barge-in** soft key is displayed on the primary line if there is a call on this line on another device. Value operation: • 0: Indicates Barge-in is disabled for the primary line. • 1: Indicates Barge-in is enabled for the primary line. This parameter is ignored in BLA mode. Ring Central Server does not support **Barge-in** . This parameter value is ignored if the selected line mode is BLA. **Note:** This parameter is supported only by Avaya J139 IP Phone, Avaya J159 IP Phone and Avaya J169/J179 IP Phone.
PRIMARY_LINE_TYPE	0	Specifies whether the phone's primary line is a private or shared line. If the primary line is a shared line, other settings that control the primary line behavior are not affected. Value operation: • 0: Indicates a private line. • 1: Indicates a shared line. **Note:** This parameter is supported only by Avaya J139 IP Phone, Avaya J159 IP Phone and Avaya J169/J179 IP Phone.

Table continues…

Parameter name	Default value	Description
PRIORITIZE_INCOMING_CALLS_LIST	0	Specifies whether visual display of incoming alerts are to be sorted when there is more than one or if they should be displayed in the order they are received. Incoming alerts can include (in priority order from high to low): incoming calls, calls parked to the user's extension, incoming calls to a monitored BLF key, calls parked to a monitored BLF key. Value operation: • 0: Sort the list of incoming alerts in the order they are received • 1: Sort the list of incoming alerts by priority **Note:** This parameter is available in • Avaya J159 IP Phone • Avaya J169/J179 IP Phone
PRIORITIZE_OWN_INCOMING_CALL	0	Specifies whether Prioritize own incoming calls over BLF calls feature is enabled or not. Valid values are: • 0 - Feature is disabled. The phone displays all calls in the order they are received. • 1 - Feature is enabled. The phone displays user’s own incoming calls and own parked calls before BLF calls and BLF parked calls.
PROCPSWD	27238	Specifies an access code to access the admin menu 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 the value in this file is intended primarily for configurations with versions of phone or if server software that do not support setting this value from the server.

Table continues…

Parameter name	Default value	Description
PROCSTAT	0	Specifies an access code to access the admin menu procedures. Value operation: • 0: Local procedures can be used (default). • 1: Local procedures cannot be used.
PROVIDE_ALTERNATE_NUM1_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed
PROVIDE_ALTERNATE_NUM2_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed
PROVIDE_BLF_CALL_PARK_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed
PROVIDE_BLF_INCOMING_CALL_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed
PROVIDE_CF_RINGTONE	0	Specifies if 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.

Table continues…

Parameter name	Default value	Description
PROVIDE_CALL_PARK_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed
PROVIDE_EXCHANGE_CALENDAR	1	Specifies if menu items for exchange calendar are displayed. Value operation: • 0: Not displayed • 1: Displayed (default)
PROVIDE_KEY_REPEAT_DELAY	0	Specifies how long a navigation button must be held down before it begins to auto-repeat, and if an option is 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. **Note:** Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description
PROVIDE_LOGOUT	1	Specifies if user can log out from the phone. Value operation: • 0: No • 1: Yes **Note:** This parameter is set to 0 in IP Office environment.
PROVIDE_NETWORKINFO_SCREEN	1	Specifies if the **Network Information** menu is displayed on the phone. Value operation: • 0: No • 1: Yes
PROVIDE_OPTIONS_SCREEN	1	Specifies if **Options & Settings** menu is displayed on phone. Value operation: • 0: No • 1: Yes
PROVIDE_PRIMARY_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed
PROVIDE_PRIORITY_ALERT_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed
PROVIDE_RING_REMINDER_RINGTONE	1	Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface. Value operation: • 0: The user menus are not displayed • 1: The user menus are displayed

Table continues…

Parameter name	Default value	Description
PROVIDE_SHARED_LINE_CONFIG	2	Specifies if the user has the ability to change Shared Line configuration using the Settings menu on the phone. Value operation: • 0: Shared lines are not displayed in settings menu. • 1: Shared lines are displayed in settings menu but all information is read-only. • 2: Shared lines are displayed in settings menu and is fully configurable. This parameter value is ignored in BLA mode. **Note:** This parameter is supported in Avaya J139 IP Phone, Avaya J159 IP Phone and Avaya J169/J179 IP Phone
PROVIDE_TRANSFER_TYPE	0	Provides the call transfer type in an Open SIP environment. Values are 0 or 1.
PSTN_VM_NUM	Null	Specifies the dialable string that is used to call into the messaging system. For example, when you press the **Message Waiting** button. **Note:** This parameter is supported when the phone is failed over.

Table continues…

Parameter name	Default value	Description
PUSHCAP	0000	Controls the modes of individual Push types. The value is a 3, 4 or 5 digit number, of which each digit controls a Push type and can have a value of 0, 1 or 2. Value operation: • 0: all Push requests are rejected for this Push type. • 1: only the Push requests with Barge mode are accepted for this Push type. • 2: the Push requests with Barge or Normal mode are accepted for this Push type. The Push types controlled by each digit (11111) are the following: • ||||+- The rightmost digit controls Top line Push requests. • |||+-- The next digit to the left controls display (WML browser) Push requests. • ||+--- The next digit to the left controls receive audio Push requests. • |+---- The next digit to the left controls transmit audio Push requests. • +----- The next digit to the left controls phonexml Push requests. **Note:** The display Push request (the WML browser) is supported only by the Avaya J169/J179 IP Phone.
PUSHPORT	80	Specifies the TCP port number to be used by the HTTP server in the phone for push. Valid values are 80 through 65,535.
Q		

Table continues…

Parameter name	Default value	Description
QLEVEL_MIN	1	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 **Note:** Avaya J129 IP Phone does not support this parameter.
R		
RECORDINGTONE_INTERVAL	15	Specifies the number of seconds between call recording tones. Valid values are from 1 to 60.

Table continues…

Parameter name	Default value	Description
RECORDINGTONE_VOLUME	0	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. **Note:** Avaya J129 IP Phone does not support this parameter.
RECOVERYREGISTERWAIT	60	Specifies a number of seconds. If no response is received to a REGISTER request within the number of seconds specified by WAIT_FOR_REGISTRATION_TIMER, the phone tries again after a randomly selected delay of 50% to 90% of the value of RECOVERYREGISTERWAIT. Valid values are from 10 to 36,000.
REDIRECT_TONE	1	Specifies the tone to play when a call goes to coverage. Valid values are from 1 to 4.

Table continues…

Parameter name	Default value	Description
REDIAL_LIST_MODE_DEFAULT	0	Specifies that if this parameter is set to Last number redial or Redial list, then it specifies default Redial button action. If this parameter is set to forced, then the Redial Softkey Options parameter will be ignored and the option to pick effect of redial button disappears from Phone UI user menu. The value operations: • **0**: Last number redial (Default) • **1**: Redial list (Default for ACO) • **2**: Last number redialed Forced • **3**: Redial list Forced **Note:** Avaya J129 IP Phone does not support this feature.
REGISTERWAIT	900	Specifies the number of seconds between re-registrations with the current server. Valid values are from 30 to 86400.
REJECT_PAGE_DURING_CALL	0	Specifies the behavior of a page target device when there is already an active call session on the device. Supported only in a Avaya Cloud Office™ or RingCentral environment when receiving a SIP INVITE with header p-rc-api-call-info: callAttributes=paging-call. This parameter enabled value has priority over AUTO_ANSWER_DURING_CALL Value operation: • 0: Do not reject the page • 1: Reject the page with SIP 486 Busy
REST_URL	0	Specifies server URL to REST service. REST URL parameter is supported with 3PPC Ring Central and Avaya Cloud Office™ environments only. REST URL parameter value is a string that follows common URL syntax, example: `"https://example.com:443/..."` This parameter is supported only in Avaya Cloud Office™.

Table continues…

Parameter name	Default value	Description
REUSETIME	60	Specifies the number of seconds that the DHCP is attempted: • With a VLAN ID of zero. True when L2Q is set to 1. • With untagged frames. True if L2Q is set to 0 or 2. • Before reusing the IP address and the associated address information, that the phone had the last time it successfully registered with a call server. While reusing an address, DHCP enters 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 and there will be no reuse.
RINGTONE_ALERTINFO	Null	Specifies a comma separated list of specific ring tones assigned to a call queue (QueueID:SelectedRingtoneID). QueueID is a string matching the call queue name, as configured in the server. SelectedRingtoneID is a numerical index of one of the ringtones known to the phone. When the server is not configured for distinct ringtones per queue, the only supported QueueID is "queue". **Note:** The parameter is supported when 3PCC_SERVER_MODE is set to 0 or 3.
RINGTONE_DEFAULT_ALTERNATE_NUM2	17	Specifies the index of the default ringtone to be used when an incoming call is from the second alternate number. Specifies the index of the default ringtone to be used when an incoming call is from the second alternate number. **Note:** This parameter is applicable only for Broadsoft environment.

Table continues…

Parameter name	Default value	Description
RINGTONE_DEFAULT_ALTERNATE_NUM1	16	Specifies the index of the default ringtone to be used when an incoming call is from the second alternate number. Specifies the index of the default ringtone to be used when an incoming call is from the second alternate number. Valid values are 1-18 or label as defined by the RINGTONES. **Note:** This parameter is applicable only for Broadsoft environment.
RINGTONE_DEFAULT_BLF_CALL_PARK	1	Specifies the index of the default ringtone to be used when a notification is received of a parked call on a BLF. Valid values are 1-18 or label as defined by the RINGTONES. **Note:** This parameter is applicable only for Open SIP servers which support the BLF feature.
RINGTONE_DEFAULT_BLF_CALL_PARK	1	Specifies the index of the default ringtone to be used when a notification that a call has been parked on the logged in extension. Valid values are 1-18 or label as defined by the RINGTONES. **Note:** This parameter is applicable only for Open SIP servers which support the BLF feature.
RINGTONE_DEFAULT_BLF_INCOMING_CALL	1	Specifies the index of the default ringtone to be used when an incoming call has been forwarded from another phone. Valid values are 1-18 or label as defined by the RINGTONES. **Note:** This parameter is applicable only for Open SIP servers which support the BLF feature.
RINGTONE_DEFAULT_CALL_FWD_RING	1	Specifies the index of the default ringtone to be used when an incoming call has been forwarded from another phone. Valid values are 1-18 or label as defined by the RINGTONES.

Table continues…

Parameter name	Default value	Description
RINGTONE_DEFAULT_CALL_PARK	1	Specifies the index of the default ringtone to be used when a notification that a call has been parked on the logged inextension. **Note:** This parameter is applicable only for Open SIP servers which support the Call Parking feature.
RINGTONE_DEFAULT_PRIORITY_ALERT	15	Specifies the index of the default ringtone to be used when an incoming priority call is received. Valid values are 1-18 or label as defined by the RINGTONES.
RINGTONE_DEFAULT_PRIMARY	1	Specifies the index of the default ringtone to be used when an incoming call is received which is not associated with any other ringtone based on the call type or a contact association.Valid values are 1-18 or label as defined by the RINGTONES.
RINGTONE_DEFAULT_RING_REMINDER	18	Specifies the index of the default ringtone to be used when an incoming call is identified as a ring reminder. **Note:** This parameter is applicable only for Open SIP servers which support this feature.
RINGTONES	Null	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 can 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.

Table continues…

Parameter name	Default value	Description
RINGTONES_UPDATE	0	Specifies if the phone queries the file server to determine if there is an updated version of each custom ring tone file each time the phone starts up or resets. Value operation: 0: Phone only tries to download ring tones with new display names (default) 1: Phone checks for updated version of each ring tone file at startup
RINGTONESTYLE	0	Specifies the style of ring tones that are offered to the user for personalized ringing when **Classic** is selected, as opposed to **Rich**. Value operation: • 0: North American ring tones are offered (default). • 1: European ring tones are offered.
RTCP_PUBLISH_ADDRESS	Null	Phone sends VQ-RTCPXR voice quality metric reports using this address in SIP PUBLISH message. This parameter works independent of RTCP Monitoring settings. This address should not have sip scheme. A valid example: user@domain.com, an invalid example: sip:user@domain.com

Table continues…

Parameter name	Default value	Description
RTCP_XR	0	Specifies whether and how VoIP Metrics Report Block as defined in RTP Control Protocol Extended Report is sent. Value operation: • 0: No Extended Report (RTCP XR) is sent. • 1: Extended Report (RTCP XR) is sent to voice monitoring servers if it is configured, and to the remote peer. • 2: Extended Report (RTCP XR) is sent only to voice monitoring servers if its configured. You can configure the voice monitoring server using the parameters RTCPMON and RTCP_PUBLISH_ADDRESS When you set RTCP_XR to value 1 or 2, then: • If RTCPMON voice monitoring server is configured, voice RTCP XR report is sent to it. • If RTCP_PUBLISH_ADDRESS is configured then VQ RTCP XR Session report (per RFC 6035) is sent to the SIP URI configured.
RTCPMON	Null	Specifies the IP or DNS address for the RTCP monitor. You can set this parameter only if the environment is not an Avaya environment. The values can range from 0 through 255 characters.
RTCPMONPERIOD	5	Specifies the interval, in seconds, for sending out RTCP monitoring reports. Valid values are from 5 to 30 seconds.
RTCPMONPORT	5,005	Specifies the RTCP monitor port number. You can set this parameter only if the environment is not an Avaya environment. The values can range from 0 through 65,535. Default is 5,005.
RTP_PORT_LOW	2048	Specifies the lower limit of the UDP port range to be used by RTP or RTCP connections. The values can range from 1024 through 65503.

Table continues…

Parameter name	Default value	Description
RTP_PORT_RANGE	40	Specifies the range or number of UDP ports available for RTP or RTCP connections This value is added to RTP_PORT_LOW to determine the upper limit of the UDP port range. The values can range from 32 through 63487.
S		
SCA<n>_BARGE_IN_ENABLED	1	Specifies whether the Barge in option is enabled or disabled for each shared line on a BroadSoft server. When it is enabled, a user can barge into a call at a different location on the <n> shared line using a line key or a soft key. <n> can be a number of 1 to 10. Value operation: • 0: Barge in is disabled for the shared line. • 1: Barge in is enabled for the shared line. Ring Central Server does not support **Barge-in** . This parameter value is ignored if the selected line mode is BLA. **Note:** These parameters are supported only by Avaya J139 IP Phone, Avaya J159 IP Phone and Avaya J169/J179 IP Phone.
SCA<n>_ENABLED	0	Specifies whether <n> shared line is enabled. <n> can be a number of 1 to 10. Value operation: • 0: Indicates disabled. • 1: Indicates enabled. **Note:** These parameters are supported only by Avaya J139 IP Phone, Avaya J159 IP Phone and Avaya J169/J179 IP Phone.

Table continues…

Parameter name	Default value	Description
SCA<n>_EXTENSION	Null	Specifies the display name of the shared line. <n> can be a number of 1 to 10. The display name used for an idle shared line can be an arbitrary label and may or may not coincide with user's login credentials. This value is optional. If not provided SCA<n>_SIPUSERID value is used. **Note:** These parameters are supported only by Avaya J139 IP Phone, Avaya J159 IP Phone and Avaya J169/J179 IP Phone.
SCA<n>_INCOMING_CALL_INDICATION_DELAYED_DEFAULT	0	Specifies the value in seconds, used by the phone to delay the displaying of call pop-pup and playing of ringtone for an incoming call. Valid values are 0–99. If you use 0, there is no delay in alerting. This parameter is not used if you select None or None forced parameter values for SCA<n>_INCOMING_CALL_INDICATION_DEFAULT.

Table continues…

Parameter name	Default value	Description
SCA<n>_INCOMING_CALL_INDICATION_DEFAULT	3	Specifies the behavior of a Shared Call Appearance Line when receiving an incoming call. N specifies a number from 1 to 10. This parameter is applicable for SCA and BLA. Value operation: • 0: None • 1: Audible • 2: Visual • 3: Both • 4: None forced • 5: Audible forced • 6: Visual forced • 7: Both forced **Note:** These parameters are supported only by Avaya J139 IP Phone, Avaya J159 IP Phone, Avaya J169/J179 IP Phone and Avaya J189 IP Phones.
SCA<n>_MAX_CALL_APPEARANCES	1	Specifies the maximum number of simultaneous calls on each specified shared line on BroadSoft server. <n> can be a number of 1 to 10 for SCA mode. This set of parameters provides independent control of the maximum number of call sessions on each shared line. This setting directly maps to the number of shared call appearances that are be displayed on the phone for this shared line. Ring Central Server supports only 1 call appearance for each shared line. Even if the value is set otherwise, the server ignores it. Values ranges from 1 to 5. **Note:** These parameters are supported only by Avaya J139 IP Phone, Avaya J159 IP Phone , Avaya J169/J179 IP Phone and Avaya J189 IP Phones.

Table continues…

Parameter name	Default value	Description
SCA<n>_PASSWORD	Null	Specifies the password used for authentication when challenged with 401 for credentials on SIP requests associated with the shared line. <n> can be a number of 1 to 10. This is a required parameter in SCA mode. The Ring Central Server ignores this value and uses authentication credentials provided in SCA<n>_SIPUSERID. **Note:** These parameters are supported only by Avaya J139 IP Phone, Avaya J159 IP Phone , Avaya J169/J179 IP Phone and Avaya J189 IP Phones.
SCA<n>_SIPUSERID	Null	Specifies the Address or Record (AOR) for each shared line. This parameter is required for both the SCA and BLA modes. <n> can be a number of 1 to 10. This parameter should only specify the handle, as the domain is specified independently. Shared lines are only supported for the same SIP domain as the primary line. **Note:** These parameters are supported only by Avaya J139 IP Phone, Avaya J159 IP Phone , Avaya J169/J179 IP Phone and Avaya J189 IP Phones.

Table continues…

Parameter name	Default value	Description
SCA<n>_USERNAME	Null	Specifies the user name to be used for authentication when challenged with 401 for credentials on SIP requests associated with the shared line. <n> can be a number of 1 to 10. This value is optional in SCA. If not provided, SCA<n>_SIPUSERID value will be used. The Ring Central Server ignores this parameter and uses authentication credentials provided in SCA<n>_SIPUSERID. **Note:** These parameters are supported only by Avaya J139 IP Phone, Avaya J159 IP Phone , Avaya J169/J179 IP Phone and Avaya J189 IP Phones.
SCA_LINE_SEIZE_DURATION	15	In SCA mode, this parameter specifies the time in seconds that a shared line stays off hook with a dial tone when the call appearance is seized before the line transitions to a failed state. In BLA mode this parameter specifies the time in seconds for the inbound subscribe duration. Values range from 5 to 600. Recommended value for the Ring Central Server is 360. **Note:** These parameters are supported only by Avaya J139 IP Phone, Avaya J159 IP Phone , Avaya J169/J179 IP Phone and Avaya J189 IP Phones in 3PCC environments.
SCEPPASSWORD	$SERIALNO	Specifies a challenge password to use with SCEP. The value of SCEPPASSWORD, if non-null, is included in a challengePassword attribute in SCEP certificate signing requests. If the value contains $SERIALNO, $SERIALNO is replaced by the value of SERIALNO. If the value contains $MACADDR, $MACADDR is replaced by the value of MACADDR without the colon separators.

Table continues…

Parameter name	Default value	Description
SCEPENCALG	0	Specifies SCEP Encryption Algorithm. Value operation: • 0: DES • 1: AES-256 **Note:** Avaya J129 IP Phone supports this parameter.
SCREENSAVER_CLOCK_ENABLE	1	Specifies whether to present clock on the screensaver. User can override the configuration in the settings menu. Value operation: • 0: Clock is not presented on screensaver. • 1: Clock is presented on screensaver.
SCREENSAVER_IMAGE	Null	Specifies the screen saver images those can be loaded from the provisioning server. Maximum five custom images can be uploaded onto the phone. Only the `.jpeg` file format is supported and the maximum file size is 256KB. Note that the image file name is case sensitive.
SCREENSAVER_IMAGE_DISPLAY	Null	Allows the administrator to display the desired screen saver image. Note that if BACKGROUND_IMAGE_SELECTABLE is set to 1 then the end user can override this setting.
SCREENSAVER_IMAGE_SELECTABLE	1	Allows the end user to select and change the screen saver images. Value operation: • 0: End user can not select and change the screen saver images from the settings menu. • 1: End user can select and change the screen saver images from the settings menu. **Note:** These parameters are supported only by the Avaya J159 IP Phone and Avaya J169/J179 IP Phone.

Table continues…

Parameter name	Default value	Description
SCREENSAVER_IMAGE_SELECTABLE	1	Allows the end user to select and change the screen saver images. Value operation: • 0: End user can not select and change the screen saver images from the settings menu. • 1: End user can select and change the screen saver images from the settings menu.
SCREENSAVER_IMAGE_SECONDARY	Null	Specifies a list of screen saver images to be used on the secondary screen. Maximum five custom images can be uploaded onto the phone. Only the `.jpeg` file format is supported and the maximum file size is 256KB. Note that the image file name is case sensitive. Example: screensaver_example1.jpg, screensaver_example2.jpeg **Note:** This parameter is supported only in Avaya J159 IP Phone
SCREENSAVER_IMAGE_DISPLAY_SECONDARY	Null	Specifies the screen saver image to be displayed on the Secondary screen. The filename will be one of the filenames listed in SCREENSAVER_IMAGE_SECONDARY. Note that if SCREENSAVER_IMAGE_SELECTABLE_SECONDARY is set to 1 then the end user may override this setting. Example: screensaver_example1.jpg **Note:** This parameter is supported only in Avaya J159 IP Phone

Table continues…

Parameter name	Default value	Description
SCREENSAVERON	240 (4 hours)	Specifies the number of minutes of idle time after which the screen saver is displayed. If an image file is downloaded based on the LOGOS parameter, it is used as the screen saver. Otherwise, the built-in Avaya one-X(TM) screen saver is 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.
SDPCAPNEG	1	Specifies if SDP capability negotiation is enabled. Value operation: 0: SDP capability negotiation is disabled. 1: SDP capability negotiation is enabled (default).
SEND_DTMF_TYPE	2	Specifies if 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)
SERVER_CERT_RECHECK_HOURS	24	Specifies the time interval in hours for rechecking expiration and revocation status of the certificates through OCSP. The valid range is from 0 to 32,767.

Table continues…

Parameter name	Default value	Description
SHARED_CALL_APPEARANCES_MODE	0	Specifies behavior of Shared Call Appearances for all Shared Lines. This parameter should only be used if SHARED_LINE_MODE is BLA Values Value operation: • 0 (Default): IPhone screen shows 1 Shared Call Appearance and Call Appearance can perform Blind Transfer only. • 1: Phone screen shows 1 Shared Call Appearance and Call Appearance can perform Blind Transfer, Consult Transfer and Conference calls. **Note:** These parameters are supported only by the Avaya J159 IP Phone, Avaya J169/ J179 IP Phone, Avaya J139 IP Phone and Avaya J189 IP Phone.
SHARED_LINE_MODE	0	Specifies whether the Bridged Line Appearance (BLA) or Shared Call Appearance (SCA) mode is used. Value operation: • 0: Indicates Shared Call Appearance mode. • 1: Indicates Bridged Line Appearance mode. **Note:** Avaya J129 IP Phone does not support this parameter.
SHOW_CALLFOR_ON_PRIMARY	0	Specifies whether incoming call pop-up messages are displayed with ‘Called for’ when a call is addressed to a primary private or shared line only. Value operation: • 0: The ‘Call for’ is not displayed. • 1: The ‘Call for’ is displayed.
SHOW_LAST_EXTENSION	0	Specifies whether to display last extension after logout. Value operation: • 0: To hide last extension after logout. • 1: To display the last extension after logout.

Table continues…

Parameter name	Default value	Description
SHORTCUT_ACTION_BLF, SHORTCUT_ACTION_CONTACT, SHORTCUT_ACTION_AUTODIAL	0	Specify the action performed if the user presses a BLF key, an Autodial key, or selects a contact on the Phone screen during an active or, in case of Call Park, an active or a held call. See the full value description in the Active call shortcut keys configuration on page 262 section. **Note:** Avaya J129 IP Phone does not support this feature.
SHORTCUT_ACTION_BLF_PARK	0	Specifies the action which is performed when the Shared Parking line is activated during an ongoing call. Valid values: • 0: Blind transfer is performed to the SP extension number. • 1: The Park FAC and the SP extension number are dialed. This option might not be available in all the environments.
SHORT_FORM_USER_ID	Null	Specifies if the users system extension number is different than the users FORCE_SIP_USERNAME and the user is monitoring other users via BLF. When the monitoring user attempts to place a call to a monitored BLF key it will prevent the J100 from displaying an incoming call for the BLF monitored user.
SIG	0	Specifies the type of software to be used by the phone 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)

Table continues…

Parameter name	Default value	Description
SIG_PORT_LOW	1024	Specifies the minimum port value for SIP signaling. Valid values are 1024 through 65503.
SIG_PORT_RANGE	64511	Specifies the range or number of SIP signaling ports. This value is added to SIG_PORT_LOW to determine the upper limit of the SIP signaling port range. Valid values are 32 through 64511).
SIGNALING_ADDR_MODE	4	Specifies the SIP controller IP address from SIP_CONTROLLER_LIST_2. This parameter is used by SIP signaling on a dual mode phone. 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. Value operation: • 4: IPv4 • 6: IPv6

Table continues…

Parameter name	Default value	Description
SIP_CONTROLLER_LIST	Null	Specifies a list of SIP controller designators, separated by commas without any spaces. The list is used on IPv4-only and dual mode phones if SIP_CONTROLLER_LIST_2 is not provided. Controller designator has the following format: `host[:port] [;transport=xxx]` where • `host` is an proxy address in dotted-decimal or DNS name format. In an Open SIP setup, only DNS format is supported. • `[:port]` is an optional port number. • `[;transport=xxx]` is an optional transport type where `xxx` can be TLS, TCP, or UDP. You can also set it to AUTO, to trigger NAPTR recording. For example, `SIP_CONTROLLER_LIST="10.138.251.56:5060;transport=tcp"`

Table continues…

Parameter name	Default value	Description
SIP_CONTROLLER_LIST_2	Null	This parameter replaces SIP_CONTROLLER_LIST for dual mode phones. It is used to select the registration address. SIP_CONTROLLER_LIST_2 is used on IPv6-only phones to provide the list of SIPv6 servers. SIPv4 servers are ignored in IPv6-only mode. Valid values are 0 to 255 characters in the dotted decimal or colon-hex format, separated by commas without any intervening spaces. The SIP Proxy list has the following format: `host[:port][;transport=xxx]` where • `host` is IP addresses in dotted-decimal format or hex format. • `[:port]` is the port number. The default value is 5,061 for TLS. • `[;transport=xxx]` is an optional transport type where `xxx` is either TLS or TCP The default value is TLS. A dual mode controller has addresses of both families within curly ({ }) brackets. This parameter should not be set and left at default. Open SIP redundancy do not support IPv6.
SIP_TIMER_T1	500	Specifies the time in milliseconds and is an estimate of the Round Trip Time (RTT). Valid values are 500 through 10000. **Note:** This parameter is supported only for 3PCC environment.

Table continues…

Parameter name	Default value	Description
SIP_TIMER_T2	4,000	Specifies the time in milliseconds and is an estimate of the maximum retransmit interval for non-INVITE requests and INVITE responses. Valid values are 2500 through 60000. **Note:** This parameter is supported only for 3PCC environment.
SIP_TIMER_T4	5,000	Specifies the time in milliseconds and is an estimate of the maximum duration for a message to remain in the network. Valid values are 500 through 10000. **Note:** This parameter is supported only for 3PCC environment.
SIP Transport UDP	0	Determines whether SIP Transport = UDP can be manually configured on the phone. Valid values are: • 0 for No • 1 for Yes **Note:** This parameter is supported for 3PCC environment.
SIPCONFERENCECONTINUE	0	Specifies if a conference call continues after the host hangs up. Value operation: • 0: Drop all parties. • 1: Continue conference **Note:** This parameter is set to 1 in IP Office environment.
SIPDOMAIN	Null	Specifies the domain name to be used during SIP registration. The value can contain 0 to 255 characters. The default value is null.

Table continues…

Parameter name	Default value	Description
SIPPORT	5,060	Specifies the port the phone opens to receive SIP signaling messages. Valid values are 1,024 through 65,535. The default value is 5,060.
SIPREGPROXYPOLICY	Simultaneous	Specifies if the phone attempts to maintain one or multiple simultaneous registrations. Value operation: Alternate: Only a single registration is attempted and maintained. Simultaneous: Simultaneous registrations is attempted and maintained with all available controllers. **Note:** You can select the alternate value for this parameter only for IP Office and 3PCC environments.
SKILLSCREENTIME	5	Specifies the duration, in seconds, that the **Skills** screen is displayed. Valid values are 0 through 60. The default value is 5. A value of 0 means that the **Skills** screen is not removed automatically when the agent logs in. **Note:** Avaya J129 IP Phoneand Avaya J139 IP Phonedo not support this parameter.
SLMCAP	0	Specifies if the SLA Monitor agent is enabled for packet capture. Value operation: • 0: Disabled (default) • 1: Enabled and payloads are removed from RTP packets • 2: Enabled and payloads are included in RTP packets • 3: Controlled from admin menu - Allows you to enable or disable of RTP packets capture using local admin procedures.

Table continues…

Parameter name	Default value	Description
SLMCTRL	0	Specifies whether the SLA Monitor agent is enabled for phone control. Value operation: • 0: Disabled • 1: Enabled • 2: Controlled from admin menu.
SLMPERF	1	Specifies whether the SLA Monitor agent is enabled for phone performance monitoring. Value operation: 0: Disabled (default) 1: Enabled
SLMPORT	50,011	Specifies the UDP port that will be opened by the SLA Monitor agent to receive discovery and test request messages. Valid values are 6,000 through 65,535. The default value is 50,011. **Note:** If default port is not used, both the SLA Mon agent and the server must be configured with the same port. This parameter impacts the phone's SLA Mon agent configuration. A corresponding configuration must also be made on the SLA Mon server `agentcom-slamon.conf` file.

Table continues…

Parameter name	Default value	Description
SLMSRVR	Null	Specifies the IP address and the port number of the SLA Mon server in the aaa.bbb.ccc.ddd:n format. Set the IP address of the SLA Mon server in the aaa.bbb.ccc.ddd format to restrict the registration of agents only to that server. Specifying a port number is optional. If you do not specify a port number, the system takes 50,011 as the default port. If the value of the port number is 0, than any port number is acceptable. The IP address must be in the dotted decimal format, optionally followed by a colon and an integer port number from 0 to 65,535. To use a non-default port, set the value in the aaa.bbb.ccc.ddd:n format, where aaa.bbb.ccc.ddd is the IP address of the SLA Mon server. **Note:** If default port is not used, both the SLA Mon agent and server must be configured with the same port. SLMSRVR impacts the phone's SLA Mon agent configuration. A corresponding configuration must also be made on the SLA Mon server `agentcom-slamon.conf` file.
SLMSTAT	0	Specifies if the SLA Monitor agent is enabled or not. Value operation: • 0: Disabled (default) • 1: Enabled in listening mode • 2: Enabled in active discovery mode, used for remote worker deployments

Table continues…

Parameter name	Default value	Description
SNMPADD	Null	Specifies a list of source IP addresses from which SNMP query messages will be accepted and processed. Addresses can be in dotted-decimal format (IPv4), colon-hex format (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.
SNMPSTRING	Null	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. Null disables SNMP.
SNTP_SYNC_INTERVAL	1440 minutes	Specifies the time interval, in minutes, during which the phone attempts to synchronize its time with configured NTP servers. Valid values are from 60 to 2,880 minutes.
SNTPSRVR	Null	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.

SOFTKEY_ACTIVE	Null	Specifies the custom soft key for the call appearance lines in an Active state. You can provide the soft key attributes and labels, which a phone displays during an active call, along with standard active call soft keys.
		For example:
		`SET SOFTKEY_ACTIVE "type=dtmf;action=##*3;label=Park"`
		`ADD SOFTKEY_ACTIVE "type=dtmf;action=*34;label=Record"`
		Note:
		Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description

SOFTKEY_HELD	Null	Specifies the custom soft key for the CA lines in a Held state. You can provide the soft key attributes and labels, which a phone displays during an incoming call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_HELD "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_SCA_HELD "type=function;action=redirect;attr1=65324;label=redirect"`

SOFTKEY_ACTIVE_PAGETARGET	Null	Specifies the custom soft key for the call appearance lines in an Active Page target state. You can provide the soft key attributes and labels, which a phone displays during a page call, along with standard soft keys.
		For example:
		`SET SOFTKEY_ACTIVE_PAGETARGET "type=dtmf;action=AnswerDigitSequence;label=Answer"`
		`ADD SOFTKEY_ACTIVE_PAGETARGET "type=function;action=endcall;label=End"`
		Note:
		Avaya J129 IP Phone does not support this feature.

SOFTKEY_BLF_ACTIVE	Null	Specifies the custom soft key for the call appearance lines in BLF Active state. You can provide the soft key attributes and labels, which a phone displays during an active BLF call, along with to standard active call soft keys.
		For example:
		`SET SOFTKEY_BLF_ACTIVE "type=dial;action=*80$attr2;label=dial"`
		`ADD SOFTKEY_BLF_ACTIVE "type=function;action=call;label=call"`
		Note:
		Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description

SOFTKEY_BLF_IDLE	Null	Specifies the custom soft key for the call appearance lines in BLF Idle state. You can provide the soft key attributes and labels which a phone displays during idle BLF line, along with standard soft keys.
		For example:
		`SET SOFTKEY_BLF_IDLE "type=function;action=call;label=call"`
		`ADD SOFTKEY_BLF_IDLE "type=function;action=pickup;label=pickup"`
		Note:
		Avaya J129 IP Phone does not support this feature.

SOFTKEY_BLF_INCOMING	Null	Specifies the custom soft key for the call appearance lines in BLF Incoming state. You can provide the soft key attributes and labels, which a phone displays during an incoming BLF call, along with standard soft keys.
		For example:
		`SET SOFTKEY_BLF_INCOMING "type=function;action=call;label=call"`
		`ADD SOFTKEY_BLF_INCOMING "type=function;action=bargein;label=Bargein"`
		Note:
		Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description

SOFTKEY_BLF_INCOMING_VISUAL	Null	Specifies the custom soft key for the call appearance lines in BLF Incoming Visual state. You can provide the soft key attributes and labels, which a phone displays during an incoming BLF call, along with standard soft keys.
		For example:
		`SET SOFTKEY_BLF_INCOMING_VISUAL "type=function;action=pickup;label=Pickup"`
		`ADD SOFTKEY_BLF_INCOMING_VISUAL "type=function;action=ignore;label=reject"`
		Note:
		Avaya J129 IP Phone does not support this feature.

SOFTKEY_BLF_OUTGOING	Null	Specifies the custom soft key for the call appearance lines in BLF outgoing state. You can provide the soft key attributes and labels, which a phone displays during a outgoing BLF call, along with addition standard soft keys.
		For example:
		`SET SOFTKEY_BLF_OUTGOING "type=dial;action=*80$attr2;label=dial"`
		`ADD SOFTKEY_BLF_OUTGOING "type=function;action=call;label=call"`
		Note:
		Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description
SOFTKEY_CONFIGURATION	0,1,2	Specifies which feature will show up on which soft key on the Avaya J129 IP Phone screens. The features are defined as follows: • 0 = Redial • 1 = Contacts • 2 = Emergency • 3 = Recents • 4 = Voicemail **Note:** Emergency calls are not supported in an Open SIP environment.

SOFTKEY_IDLE	Null	Specifies the custom soft key for the call appearance lines in an Idle state. You can provide the soft key attributes and labels, which a phone displays during idle, along with standard soft keys.
		For example:
		`SET SOFTKEY_IDLE "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_IDLE "type=function;action=emergency;label=emergency2"`
		Note:
		Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description

SOFTKEY_INCOMING	Null	Specifies the custom soft key for the call appearance lines in an Incoming state. You can provide the soft key attributes and labels, which a phone displays during an incoming call, along with standard soft keys.
		For example:
		`SET SOFTKEY_INCOMING "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_INCOMING "type=function;action=decline;label=reject"`
		Note:
		Avaya J129 IP Phone does not support this feature.

SOFTKEY_INCOMING_VISUAL	Null	Specifies the custom soft key for the call appearance lines in an Incoming Visual state. You can provide the soft key attributes and labels, which a phone displays during an incoming call, along with standard soft keys.
		For example:
		`SET SOFTKEY_INCOMING_VISUAL "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_INCOMING_VISUAL "type=function;action=redirect;attr1=65324;label=divert"`
		Note:
		Avaya J129 IP Phone does not support this feature.

Table continues…

Parameter name	Default value	Description

SOFTKEY_OUTGOING	Null	Specifies the custom soft key for the call appearance lines in an Outgoing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_OUTGOING "type=function;action=endcall;label=drop"`
		`ADD SOFTKEY_OUTGOING "type=function;action=endcall;label=finish"`
		Note:
		Avaya J129 IP Phone does not support this feature.

SOFTKEY_SCA_ACTIVE	Null	Specifies the custom soft key for the shared lines in an Active state. You can provide the soft key attributes and labels, which a phone displays during an active call, along with standard active call soft keys.
		For example:
		`SET SOFTKEY_SCA_ACTIVE "type=dtmf;action=##*3;label=Park"`
		`ADD SOFTKEY_SCA_ACTIVE "type=dtmf;action=*34;label=Record"`

SOFTKEY_SCA_ACTIVE_PAGE TARGET	Null	Specifies the custom soft key for the shared lines in an Active Page target state. You can provide the soft key attributes and labels, which a phone displays during a page call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_ACTIVE_PAGETARGET "type=dtmf;action=AnswerDigitSequence;label=Answer"`
		`ADD SOFTKEY_SCA_ACTIVE_PAGETARGET "type=function;action=endcall;label=End"`

Table continues…

Parameter name	Default value	Description

SOFTKEY_SCA_IDLE	Null	Specifies the custom soft key for the shared lines in an Idle state. You can provide the soft key attributes and labels, which a phone displays during idle, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_IDLE "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_SCA_IDLE "type=function;action=emergency;label=emergency2"`

SOFTKEY_SCA_INCOMING	Null	Specifies the custom soft key for the shared lines in an Incoming state. You can provide the soft key attributes and labels, which a phone displays during an incoming call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_INCOMING "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_SCA_INCOMING "type=function;action=decline;label=reject"`

SOFTKEY_SCA_INCOMING_VISUAL	Null	Specifies the custom soft key for the shared lines in an Outgoing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.

SOFTKEY_SCA_OUTGOING	Null	Specifies the custom soft key for the shared lines in an Outgoing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_OUTGOING "type=function;action=endcall;label=drop"`
		`ADD SOFTKEY_SCA_OUTGOING "type=function;action=endcall;label=finish"`

Table continues…

Parameter name	Default value	Description

SOFTKEY_SCA_HELD	Null	Specifies the custom soft key for the shared lines in a Held state. You can provide the soft key attributes and labels, which a phone displays during an incoming call, along with standard soft keys.
		For example:
		`SET SOFTKEY_SCA_HELD "type=function;action=newcall;label=call"`
		`ADD SOFTKEY_SCA_HELD "type=function;action=redirect;attr1=65324;label=redirect"`

SOFTKEY_SCA_CONFERENCE_DIALING	Null	Specifies the custom soft key for the call shared lines in a Conference Dialing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_CONFERENCE_DIALING "type=function;action=clear;label=drop"`
		`ADD SOFTKEY_CONFERENCE_DIALING "type=function;action=endcall;label=finish"`

SOFTKEY_SCA_CONFERENCE_OUTGOING	Null	Specifies the custom soft key for the shared lines in a Conference Outgoing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_CONFERENCE_OUTGOING "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_CONFERENCE_OUTGOING "type=function;action=clear;label=finish"`

Table continues…

Parameter name	Default value	Description

SOFTKEY_SCA_CONFERENCE_CONSULT	Null	Specifies the custom soft key for the shared lines in a Conference Consult state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_CONFERENCE_CONSULT "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_CONFERENCE_CONSULT "type=function;action=endcall;label=finish"`

SOFTKEY_SCA_CONFERENCE_ACTIVE	Null	Specifies the custom soft key for the shared lines in a Conference Active state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_CONFERENCE_ACTIVE "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_CONFERENCE_ACTIVE "type=function;action=endcall;label=finish"`

SOFTKEY_SCA_TRANSFER_DIALING	Null	Specifies the custom soft key for the shared lines in a Transfer Dialing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_TRANSFER_DIALING "type=function;action=clear;label=drop"`
		`ADD SOFTKEY_TRANSFER_DIALING "type=function;action=endcall;label=finish"`

Table continues…

Parameter name	Default value	Description

SOFTKEY_SCA_TRANSFER_OUTGOING	Null	Specifies the custom soft key for the shared lines in a Transfer Outgoing state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_TRANSFER_OUTGOING "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_TRANSFER_OUTGOING "type=function;action=clear;label=finish"`

SOFTKEY_SCA_TRANSFER_CONSULT	Null	Specifies the custom soft key for the shared lines in a Transfer Consult state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.
		For example:
		`SET SOFTKEY_TRANSFER_CONSULT "type=function;action=cancel;label=drop"`
		`ADD SOFTKEY_TRANSFER_CONSULT "type=function;action=endcall;label=finish"`

SPACES_ACCESS_MODE	1	Specifies the authentication mode that can be used by the phone when connecting to Avaya Spaces. The options are: • 0: Disabled, all Avaya Spaces features via APIs are disabled. • 1: Guest only, Avaya Spaces feature can be accessed by guest/anonymous authentication only. Connections to Avaya Spaces uses the embedded public certificates and any certificates defined in the TRUSTCERTS. It ignores ENABLE_PUBLIC_CA_CERTS. **Note:** This parameter is not supported on Avaya J129 IP Phone.

Table continues…

Parameter name	Default value	Description
SPACES_DIRECT_NUMBER_DEFAULT	Null	You can define a direct number to use when attempting a call to Avaya Spaces. If the user does not select an Avaya Spaces direct number then this defined direct number is used. The value is a dialable string, length can be up to 32 characters. Can contain the following: 0 to 9 digits, minus (-), parenthesis ((), comma (,), pound (#), asterisk (*), plus (+). **Note:** This parameter is not supported on Avaya J129 IP Phone.
SPACES_DIRECT_NUMBER_PROVIDE	1	Specifies if the end user is allowed to select a direct number for a voice call to Avaya Spaces. The options are: • 0: Hide, user is not allowed to select a direct number for a voice call to Avaya Spaces. Any previously selected direct number by the end user is cleared. If SPACES_DIRECT_NUMBER_DEFAULT is not defined or found to not exist as a valid Direct Number, the user sees an error and warning pop-up on the phone screen. The phone does not display the Call soft key for the Avaya Spaces feature. • 1: Show, user is allowed to select a direct number for a voice call to Avaya Spaces. **Note:** WLAN_COUNTRY is used to determine the location of the phone. The phone displays phone numbers based on this location. If you set the parameter WLAN_COUNTRY to a country that does not exist in the list of numbers provided by Avaya Spaces, then the phone number of the US is shown. This parameter is not supported on Avaya J129 IP Phone.

Table continues…

Parameter name	Default value	Description
SPEAKERSTAT	2	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. **Note:** Avaya J129 IP Phone does not support this feature.
SSH_ALLOWED	0	Specifies if SSH is supported. Value operation: 0: Disabled 1: Enabled 2: Configured using local craft procedure. When this mode is configured, then by default the SSH server is disabled.
SSH_BANNER_FILE	Null	Specifies the file name or URL for a custom SSH banner file. If the value is null, English banner is used for SSH. The value can contain 0 to 255 characters.
SSH_IDLE_TIMEOUT	10	Specifies the idle time in minutes after which an SSH connection is terminated Valid values are 0 through 32,767. A value of 0 means that the connection will not be terminated.

Table continues…

Parameter name	Default value	Description
STUN_SERVER_ADDRESS	Null	This is the basic STUN parameter defining the STUN server address. Other parameters listed below will be ignored if this parameter is not set. The valid value is an IPv4 address in the dotted decimal format or a FQDN. **Note:** If specified as an IPv4 address, the STUN server port will default to 3478. It is applicable only when 3PCC_SERVER_MODE=0 or 3PCC_SERVER_MODE=2 and ENABLE_3PCC_ENVIRONMENT=1 The following characters are allowed: • 0 – 9 • a – z • A – Z • dot (“.”) For example, `SET STUN_SERVER_ADDRESS 192.168.161.54`
STUN_UDP_INITIAL_TIMEOUT_MSEC	500	Determines the initial timeout, in milliseconds, to wait for a Response to a STUN Request sent over UDP. The timeout value is internally doubled after each (re)transmission. Valid values are positive integers from 500 (0,5 sec) to 3000 (3 sec).
STUN_UDP_MAX_TRANSMISSIONS	7	Sets the number of times the phone will transmit a STUN Request until a Response is received, after which the Request will be treated as failed. Valid values are positive integers from 1 to 7.

Table continues…

Parameter name	Default value	Description
STUN_UDP_MAX_MEDIA_TRANSMISSIONS	3	Specifies the number of times the phone transmits a STUN Request to get NAT bindings for the phone's RTP or RTCP IP address and ports. Retransmissions continue until a response is received, or until the total number of requests has been sent. Initial timeout, in milliseconds, to wait for a Response to a STUN Request sent over UDP for media is 500 msec. The timeout value is internally doubled after each (re)transmission. Valid values are 1 through 4.
SUBSCRIBE_LIST_NON_AVAYA	Null	Specifies comma separated list of event packages to subscribe to after registration. Possible values are: reg, dialog, mwi, ccs, message-summary which is identical to mwi, avaya-ccs-profile which is identical to ccs. The values are case insensitive. For IPO the recommended value shall be reg, message-summary, avaya-ccs-profile.
SUBSCRIBE_SECURITY	0	Specifies the use of SIP or SIPS for subscriptions. Value operation: 0: The phone uses SIP for both the request URI and the contact header . 1: The phone uses SIPS for both the request URI and the contact header . TLS is on . 2: SES or PPM does not show a FS-phoneData FeatureName with a Feature Version of 2 in the response to the getHomeCapabilities request

Table continues…

Parameter name	Default value	Description
SUBSCRIBELIST	Null	Specifies a list of URIs to which the phone will send a subscribe message after the phone successfully registers with a call server, or when a subscribe push request is received with a type attribute all. The message is an HTTP GET for the URI with the phone's MAC address, extension number, IP address and model number appended as query values) The list can contain up to 255 characters. Values are separated by commas without any intervening spaces. If the value is set to null, subscribe messages are not sent.
SYMMETRIC_RTP	1	Specifies if the phone must discard received RTP datagrams if their UDP source port number is not the same as the UDP destination port number included in the RTP datagrams of that endpoint. Value operation: 0: Ignore the UDP source port number in received RTP datagrams. 1: Discard received RTP datagrams (default).
SYSLOG_ENABLED	0	Specifies if Syslog messages must be send or not. Value operation: 0: Sending Syslog messages is disabled (default) 1: Sending Syslog messages is enabled

Table continues…

Parameter name	Default value	Description
SYSLOG_LEVEL	4	Specifies the severity level of syslog messages. Events with the selected severity level and above will be logged. the lower numeric severity values correspond to higher severity levels. Value operation: • 3: Error, Critical, Alert and Emergency events are logged • 4: Warning, Error, Critical, Alert and Emergency events are logged (Default) • 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.
SYSTEM_LANGUAGE	Mlf_English.xml	Contains the name of the default system language file used in the phone. The filename should be one of the files listed in the LANGUAGES parameter. If no filename is specified, or if the filename does not match one of the LANGUAGES values, the phone uses the built-in English text strings. Valid values range from 0 through 32 ASCII characters. Filename must end in `.xml`.
T		
TCP_KEEP_ALIVE_INTERVAL	10	Specifies the number of seconds that the telephone waits before re-transmitting a TCP keep-alive (TCP ACK) message. Valid values are from 5 to 60.

Table continues…

Parameter name	Default value	Description
TCP_KEEP_ALIVE_STATUS	1	Specifies if the phone sends TCP keep alive messages. Value operation: 0: Keep-alive messages are not sent 1: Keep-alive messages are sent (default)
TCP_KEEP_ALIVE_TIME	60	Specifies the number of seconds that the telephone waits before sending out a TCP keep-alive (TCP ACK) message. Valid values are from 10 through 3,600
TEAM_BUTTON_REDIRECT_INDICATION	0	Specifies if the redirection indication must be shown on a team button on the monitored station, if it is not a redirect destination of the monitored station. Value operation: 0: Disabled. The redirect indication is shown only on a monitoring station which is redirection destination. 1: Enabled. The redirection indication is displayed on all monitoring stations **Note:** Avaya J129 IP Phoneand Avaya J139 IP Phone do not support Team Button feature.
TEAM_BUTTON_RING_TYPE	1	Specifies the alerting pattern to use for team buttons. Valid values are 1 through 8. The default value is 1. **Note:** Avaya J129 IP Phoneand Avaya J139 IP Phone do not support Team Button feature.

Table continues…

Parameter name	Default value	Description
TIMEFORMAT	0	Specifies the format for time displayed in the phone. The TIMEFORMAT parameter is value is applied on the very first installation, and after resetting parameters to defaults and when 3rd party servers don't backup the settings. Value operation: • 0: uses ADMINTIMEFORMAT • 1: AM or PM format • 2: 24 hour format
TLS_VERSION	0	Specifies the TLS version used for all TLS connections (except SLA monitor agent) Value operation: 0: TLS versions 1.0 and 1.2 are supported. 1: TLS version 1.2 only is supported.
TLSDIR	Null	Specifies the path to the configurations and data files in HTTPS GET operations during device bootup. This path is relative to the root of the HTTPS file server, to the directory in which the device configuration and date files are stored. If $MACADDR and/or $MODEL4 and/or $SERIALNO macro is present in the configured path then such macro is replaced with its actual value. Valid values can contain 0 to 127 ASCII characters, without any spaces.
TLSPORT	443	Specifies the TCP port used for HTTPS file downloads from non-Avaya servers. Valid values are from 0 to 65,535.
TLSSRVR	Null	Specifies zero or more HTTPS server IP addresses, which is used to download configuration script files. The IP addresses can be specified in dotted-decimal, or DNS name format separated by commas without any intervening spaces. Valid values contain 0 to 255 ASCII characters, including commas. This parameter can also be changed through LLDP.

Table continues…

Parameter name	Default value	Description
TLSSRVRID	1	Specifies how a phone evaluates a certificate trust. Value operation: • 0: Identity matching is not performed. • 1: The certificate is trusted only if the identity used to connect to the server matches the certificate identity, as per Section 3.1 of RFC 2818. For SIP-TLS connections, an additional check is performed to validate the SIP domain identified in the certificate, as per RFC 5922. The parameter is configured through the `46xxsettings.txt` file.
TPSLIST	Null	Specifies a list of URI authority components (optionally, including scheme and path components) to be trusted. A URI received in a push request is only used to obtain push content, if it matches one of these values. The list can contain up to 255 characters. Values are separated by commas without any intervening spaces. If the value of TPSLIST is null, push is disabled.
TRUSTCERTS	Null	Specifies a list of names of files that contain copies of CA certificates (in PEM format) that are 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.
U		

Table continues…

Parameter name	Default value	Description
UPDATE_DIALED_NUMBER_ON_ANSWER	0	Specifies whether displayed dialed number is updated or not based on the number provided in 200 OK after an answer. Value operation: • 0: Displayed dialed number is not updated based on 200 OK received after answer (default) • 1: Displayed dialed number is updated based on the number provided in 200 OK after answer..
USBPOWER	2	Controls USB power when power is provided to the USB interface. Value operation: • 0: Turn off USB power regardless of power source. • 1: Turn on USB power only if Aux powered. • 2: Turn on USB power regardless of power source. • 3: Turn on USB power if Aux powered or PoE Class 3 power. **Note:** This parameter is supported only in Avaya J159 IP Phone
USE_CONTACT_IN_REFERTO	1	Specifies which transfer target address should be used in Refer-To a header of REFER SIP request on attended transfer. Value operation: • 0: Use CONTACT URI of the transfer target in Refer-To header of REFER SIP request. • 1: Use TO URI of the transfer target in Refer-To header of REFER SIP request.
USE_EXCHANGE_CALENDAR	0	Specifies whether the Calendar synchronizes with the Microsoft Exchange. Value operation: • 0: To disable synchronization. • 1: To enable synchronization.

Table continues…

Parameter name	Default value	Description
USE_QUAD_ZEROES_FOR_HOLD	0	Specifies how Hold will be signaled in SDP. Value operation: • 1: “a=directional attributes" will be used • 0: "c=0.0.0.0" will be used
USER_STORE_URI	Nulll	Specifies the URI path of IP Office for storing user data. **Note:** If the value of this parameter is set to null, then the addition, deletion, and modification of **Contacts** is disabled.
UUIDISPLAYTIME	10	Specifies the duration, in seconds, that the **UUI Information** screen is be displayed. Valid values are from 5 to 60. **Note:** Avaya J129 IP Phoneand Avaya J139 IP Phonedo not support this feature.
V		

Table continues…

Parameter name	Default value	Description
VLANSEP	1	Specifies whether VLAN separation is enabled by the built-in Ethernet switch while the phone is tagging frames with a non-zero VLAN ID. When VLAN separation is enabled, only frames with a VLAN ID that is the same to the VLAN ID used by the phone (as well as priority-tagged and untagged frames) is forwarded to the phone. Also, if the value of PHY2VLAN is non-zero, only frames with a VLAN ID that is the same to the value of PHY2VLAN (as well as priority-tagged and untagged frames) is forwarded to the secondary (PHY2) Ethernet interface. 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. Value operation: 0: Disabled. 1: Enabled if L2Q, L2QVLAN and PHY2VLAN are set appropriately (default). **Note:** Avaya J129 IP Phonedoes not support this parameter.
VLANSEPMODE	0 1 for J129	Specifies whether full VLAN separation is 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 and PHY2VLAN have non-zero values, L2Q is auto (0) or (1) tagging.PHY2PRIO is not supported when VLANSEPMODE is 1. Value operation: • 0: Disabled • 1: Enabled **Note:** This parameter is configured through the settings file.

Table continues…

Parameter name	Default value	Description
VLANTEST	60	Specifies the number of seconds that the phone waits prior to failing back to a different VLAN ID if no response is received from the DHCP server. Valid values are 0 through 999. A value of zero means that DHCP tries with a non-zero VLAN ID forever. **Note:** This parameter is configured through: • Settings file • A name equal to value pair in DHCPACK message
W		
WAIT_FOR_CALL_OPERATION_RESPONSE	3	Specifies the time in seconds before providing the user a notification that there is a call operation in progress. This parameter is applicable to all server environments. When the user goes off-hook, the phone sends an invite. If there is no response from the proxy for three (default value) seconds, the phone will display the notification. Valid values range from 0 to 4. • 0: the notification is disabled • 1 – 4: the number of seconds before the popup display
WAIT_FOR_INVITE_RESPONSE_TIMEOUT	60	Specifies the maximum number of seconds that the phone waits for another response after receiving a SIP 100 Trying response. Valid values are 30 through 180.
WAIT_FOR_REGISTRATION_TIMER	32	Specifies the number of seconds that the phone waits 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 3,600.

Table continues…

Parameter name	Default value	Description
WAIT_FOR_UNREGISTRATION_TIMER	32	Specifies the number of seconds the phone waits before assuming that an un-registration request is complete. Un-registration includes termination of registration and all active dialogs. Valid values are 4 through 3,600.
WARNING_FILE	Null	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.
WBCSTAT	1	Specifies whether a wideband codec indication is displayed when a wideband codec is used. Value operation: 0: Disabled 1: Enabled **Note:** J129 does not support this parameter
WEB_ADMIN_PASSWORD	27238	Specifies the password to access the phone through a web browser as an administrator. The value set from the web server interface has a higher priority than that of the Settings file. If the Web admin password is changed using the web server, then the web admin password set through settings file is not used until either the web admin password is set to default through the phone admin menu or the phone is reset to default. Valid values are from 8 to 31 alphanumeric characters including upper, lower and special characters.
WEB_HTTP_PORT	80	Specifies the port on which the Web Server running on the phone will be accessed using HTTP. Valid values are 0, 80, 1024 to 65,535.

Table continues…

Parameter name	Default value	Description
WEB_HTTPS_PORT	443	Specifies the port on which the Web Server running on the phone will be accessed using HTTPS. Valid values are 443, 1024 to 65,535.
WEBSERVER_ON_HTTP	1	Specifies whether HTTP access to the web server is enabled or disabled. To access WEB Server using HTTP set ENABLE_WEBSERVER and WEBSERVER_ON_HTTP to 1. To access WEB Server using HTTPS set ENABLE_WEBSERVER to 1 and use factory installed identity certificate or install the identity certificates using WEB/SCEP/ PKCS12 file download. Value operation: • 0: Web Server is not accessible through HTTP. • 1: Web Server is accessible through HTTP.
WLAN_MAX_AUTH_FAIL_RETRIES	3	Specifies the number of times the phone will retry a secure connection upon receiving (possibly successive) auth failures. The valid values range from 0 to 4.
WMLEXCEPT	Null	Specifies zero or more IP addresses or domains for which the HTTP proxy server specified by WMLPROXY will not be used. The values are separated by commas without any intervening spaces. The value can contain up to 255 characters. Only Avaya J169/J179 IP Phones support this parameter.

Table continues…

Parameter name	Default value	Description
WMLHOME	Null	Specifies the URL of a WML page to be displayed by default in the WML browser and if the **Home** soft key is selected in the browser. The allowed value contains not more than one URL of up to 255 characters. **Note:** If the value is set to default, the WML browser is disabled. Only Avaya J169/J179 IP Phones support this parameter.
WMLIDLETIME	10	Specifies the idle time in minutes after which the web page set as the value of WMLIDLEURI will be displayed. The allowed value is a positive integer from 1 to 999. **Note:** If WMLIDLEURI is set to null, the web page will not be displayed when the phone is idle. Only Avaya J169/J179 IP Phones support this parameter.
WMLIDLEURI	Null	Specifies the URL for a WML page to be displayed when the telephone has been idle for the time interval in minutes specified by the WMLIDLETIME parameter. The allowed value contains not more than one URL of up to 255 characters. Only Avaya J169/J179 IP Phones support this parameter.
WMLPORT	8080	Specifies the TCP port number of the HTTP proxy server set as the WMLPROXY value. Allowed values are from 0 to 65,535. Only Avaya J169/J179 IP Phones support this parameter.

Table continues…

Parameter name	Default value	Description
WMLPROXY	Null	Specifies zero or one address for an HTTP proxy server that is used by the WML browser, and by the Weather and World Clock applications on the 9621, 9641 and 9670. The address can be in dotted-decimal (IPv4), or DNS name format, separated by commas without any intervening spaces. The value can contain up to 255 characters. Only Avaya J169/J179 IP Phones support this parameter.
X		
XSI_CHANNEL_DURATION	60	Specifies the time duration in minutes for XSI event channel. The phone will ask 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. Valid values are 60 to 1440 minutes.
XSI_HEARTBEAT	15	Specifies the interval in seconds to send heartbeat messages over Comet HTTP connection to XSP server of BroadWorks. Valid values are 1 to 999 seconds. **Note:** XSI_HEARTBEAT should equal to Broadsoft eventTimeout/2. The EventTimeout duration can be viewed in BroadSoft web interface.
XSI_URL	Null	Specifies BroadWorks Xtended Service Platform (XSP) server FQDN / IP address, HTTP or HTTPS mode and port. If the port is not defined, 80 is used for HTTP and 443 for HTTPS by default.

List of Wi-Fi configuration parameters

Parameter Name	Default Value	Description
WIFISTAT	`1`	Specifies the network interface to be used for network connectivity. Value operation: • `0`: Phone connects to only Ethernet network. • `1`: Phone connects to Ethernet network, unless manually switched to Wi-Fi • `2`: Phone connects to the Wi-Fi network with the SSID defined in the `46xxsettings.txt` parameter WLAN_ESSID
ENABLE_NETWORK_CONFIG_BY_USER	`1`	Enables network configuration to be modified by the user. Value operation: • `0`: Disabled • `1`: Enabled
WLAN_ESSID	N/A	Specifies the wireless network to be used. The name of the SSID ranges up to 32 characters.
WLAN_SECURITY	none	Specifies the security standard to be used for the wireless network. Value operation: • none: No security standard is defined. • `wep`: WEP security standard is defined. • `wpa2psk`: WPA2 security standard with pre-shared key is defined. • `wpapsk`: WPA security standard with pre-shared key is defined. • `wpa2e`: WPA enterprise security standard is defined.

Table continues…

Parameter Name	Default Value	Description
WEP_DEFAULT_KEY	N/A	Specifies the index of WEP default key. Value operation: • 1 • 2 • 3 • 4
WLAN_COUNTRY	US	Specifies the ISO country code representing the Wi-Fi regulatory domain.
WLAN_ENABLE_80211D	0	Enables the phone to configure its Wi-Fi regulatory domain to match the 802.11d. Value operation: • 0: Disable • 1: Enable
WLAN_MAX_AUTH_FAIL_RETRIES	3	Specifies the number of times the phone will retry a secure connection upon receiving (possibly successive) auth failures. The valid values range from 0 to 4.
WEP_KEY_LEN	128 bit	Specifies the length of the WEP key. Value operation: • 40 bit • 64 bit • 128 bit

Table continues…

Parameter Name	Default Value	Description
WLAN_PASSWORD	N/A	Specifies the pre-configured Wi-Fi network password. This parameter is applicable if the WIFISTAT is enabled and WLAN_SECURITY is `wpa2psk`, or WLAN_SECURITY is `wpa2e`, WLAN_WPA2E_EAP_METHOD is `PEAP` and WLAN_WPA2E_EAP_PHASE2 is `MSCHAPV2`. The password must be from 8 to 63 characters. Note that the space and ASCII 0x20 are not supported.
WLAN_WPA2E_EAP_PHASE2	N/A	Specifies the pre-configured Wi-Fi network 802.1x phase 2 Method. This parameter is only applicable when WIFISTAT enables Wi-Fi and WLAN_SECURITY is wpa2e and WLAN_WPA2E_EAP_METHOD is PEAP. Value operation: • none- No phase 2 authentication (Default, but not currently supported) • MSCHAPV2 : set to this value for forward compatibility **Note:** Avaya J129 IP Phone, Avaya J159 IP Phone, and Avaya J179 IP Phone support a pluggable Wi-Fi/BT module

Table continues…

Parameter Name	Default Value	Description
WLAN_WPA2E_ANONYMOUS_IDENTITY	Null	Specifies the pre-configured Wi-Fi network 802.1x anonymous identity. This parameter is only applicable when WIFISTAT enables Wi-Fi and WLAN_SECURITY is wpa2e and WLAN_WPA2E_EAP_METHOD is PEAP and WLAN_WPA2E_EAP_PHASE2 is MSCHAPV2. The value can contain 1 to 32 characters; Valid characters are: A-Z, a-z, 0-9, and the following: *.-!$%&'()+,:;/\=@~ The space character, ASCII 0x20, is NOT supported. **Note:** Avaya J129 IP Phone, Avaya J159 IP Phone, and Avaya J179 IP Phone support a pluggable Wi-Fi/BT module
WEP_KEY_1 to WEP_KEY_4	N/A	Specifies the name of the WEP key. The name of the 40 bit key and 128 bit key are of 10 hex digits and 26 hex digits respectively.
WLAN_WPA2E_EAP_METHOD	`PEAP`	Specifies the pre-configured 802.1x EAP method. This parameter is applicable if WIFISTAT parameter is enabled and WLAN_SECURITY is set as `wpa2e`. Value operation: • `PEAP` • `TLS`

Table continues…

Parameter Name	Default Value	Description
WLAN_WPA2E_IDENTITY	N/A	Specifies the 802.1x name of pre-configured Wi-Fi network. This parameter is applicable if WIFISTAT parameter is enabled and WLAN_SECURITY is set as `wpa2e`. The name must be from one to 32 characters. Note that the space character and ASCII 0x20 are not supported.
WLAN_WPA2E_ANONYMOUS_IDENTITY	N/A	Specifies the 802.1x anonymous name of pre-configured Wi-Fi network. This parameter is applicable if WIFISTAT parameter is enabled, WLAN_WPA2E_EAP_METHOD is set to `PEAP` and WLAN_SECURITY is set as `wpa2e`. The name must be from one to 32 characters. Note that the space character and ASCII 0x20 are not supported.
WLAN_L2QAUD	`6`	Specifies the layer 2 priority value for audio frames generated by the telephone. Valid value is from 0 to 7.
WLAN_DSCPAUD	`46`	Specifies the layer 3 Differentiated Services (DiffServ) Code Point for audio frames generated by the telephone. Valid value is from 0 to 63.
WLAN_L2QSIG	`3`	Specifies the layer 3 Differentiated Services (DiffServ) Code Point for audio frames generated by the telephone. Valid value is from 0 to 63.
WLAN_DSCPSIG	`34`	Specifies the layer 3 Differentiated Services (DiffServ) Code Point for signaling frames generated by the telephone. Valid value is from 0 to 63.

Downloadable directory syntax

In generic Open SIP and Asterisk environments, upload the global contacts of your organization to the phones by using the downloadable directory feature. Update the directory file with the required contacts and store it in the file server.

Following is the criteria to update the directory file.

- You can save maximum 200 contacts in the .xml file.
- You can have 31 characters for the first name and last name of each contact.
- You can save maximum 4 phone numbers for each contact.

Important:

Save the Directory file in .xml format.

Use the following syntax to upload the contacts in phones.

```
<DirectoryEntry>
<LastName>Lastname1Lastname1Lastname11234</LastName>
<FirstName>Firstname1Firstname1Firstname11234</FirstName>
                  <PhoneNumbers>
                       <Phone>
                              <Number>6139675040212121212</Number>
                              <Type>Work</Type>
                        </Phone>
                        <Phone>
                               <Number>61396750402121212l</Number>
                              <Type>Home</Type>
                        </Phone>
       <Phone>
                               <Number>61396750402121212l</Number>
                              <Type>Mobile</Type>
                        </Phone>
                        <Phone>
                               <Number>61396750402121212l</Number>
                              <Type>Other</Type>
                        </Phone>
               </PhoneNumbers>
</DirectoryEntry>
```

Example of a complete .xml file

```
<IPPhoneDirectory>
<!-- Contact with lastname, firstname and three phone numbers with different types --
><DirectoryEntry>
<LastName>Lastname1Lastname1Lastname11234</LastName>
<FirstName>Firstname1Firstname1Firstname11234</FirstName>
                  <PhoneNumbers>
                       <Phone>
                              <Number>6139675040212121212</Number>
                              <Type>Work</Type>
                        </Phone>
                        <Phone>
                               <Number>61396750402121212l</Number>
                              <Type>Home</Type>
                        </Phone>
       <Phone>
                               <Number>61396750402121212l</Number>
                              <Type>Mobile</Type>
                        </Phone>
                        <Phone>
```


Comments on this document? infodev@avaya.com

```
                                <Number>613967504021212121</Number>
                               <Type>Other</Type>
                        </Phone>
                </PhoneNumbers>
</DirectoryEntry>
</IPPhoneDirectory>
```

Soft key parameter values

This section contains the full list of soft key parameter values and their attributes.

Each soft key has a set of attributes that can be configured for the soft key parameter:

- `Type`: key type, a mandatory value, the list of available values depend on the Call Appearance States.
- `Action`: value depends on the type and the Call Appearance States selected.
- `Label`: soft key label, optional value. The value accepts non-Latin symbols.

Note:

If you do not specify the `Label` value, the default built-in Label is used for the `Type=Function`, and the `Action` value is used for all other `Type`.

Following is the syntax for the soft key parameter:

```
SET SOFTKEY_<state> "type=<type>;action=<action>;label=<label>"
```

To add multiple soft keys use the ADD command.

For the full list of allowed values, refer to the table below. For additional settings of the SOFTKEY parameter, refer to the **Additional parameters** column.

Primary Call Appearance State	Soft key setting	Action	Label	Additional parameters
All the Call Appearance States	`Type=Blank`	Null	Null	
Active **Active Page Target**	`Type=DTMF`	Allows: • 0 to 9 • Letters (a to z) • Asterisk (*) • Pound (#)	String value. Allows any UNICODE symbol, except for the following: • Semicolon (;) • Comma (,) • Quote (“) • Equal (=)	
Active	`Type=Dial`			

Table continues…

Primary Call Appearance State	Soft key setting	Action	Label	Additional parameters
ActiveConference ActiveConference Consult	Type=Function	Hold	• Pipe (|) • Lesser than (<) • Greater than (>) • Forward slash (/) • Ampersand (&)	
Active		Transfer		
Active **Active Page Target** **OutgoingTransfer DialingConference ActiveConference Dialing**		End Call		
Active **Idle** **Incoming** **Held** **Conference Active**		New Call		
Active		Conference		
Active **Held** **Active Page Target**		Details		
Idle **Dialtone** **Dialing**		Redial		
Idle		Emergency		
Incoming **Incoming Visual**		Decline		

Table continues…

Primary Call Appearance State	Soft key setting	Action	Label	Additional parameters

Incoming
Incoming Visual
		Redirect		Attr1: allows valid SIP URI characters such as: leading +, asterisk (*), pound (#), at (@), comma (,), minus (-), underscore (_), 0–9, a-z, A-Z. Currently, only one Redirect soft key is supported.
				For example:
				`Attr1=some_address`
				`Attr1=some_address@domain.com`
				`Attr1=+16135555555@domain.com`
				`Attr1=+16135555555`
				`Attr1=16135555555`
				`Attr1=*088063#`
				If you do not set the value per the defined rules, the Attr1 is undefined. However, the Redirect soft key appears.

Incoming **Incoming Visual**		Answer		
IncomingIncoming Visual		Ignore		
Held		Resume		
Conference Active		Add		
Conference ActiveConference Consult		Join		
Conference Active		Drop		

Table continues…

Primary Call Appearance State	Soft key setting	Action	Label	Additional parameters
Conference Consult **Conference Outgoing** **Transfer Dialing** **Transfer Consult**		Cancel		
Dialing **Transfer DialingConference Dialing**		Clear		

SCA Call Appearance State	Soft key setting	Action	Label	Additional parameters
All the Call Appearance States	`Type=Blank`	Null	Null	
Idle **Active** **Outgoing**	`Type=Dial`	Allows: • 0 to 9 • Letters (a to z) • Asterisk (*) • Pound (#)	String value. Allows any UNICODE symbol, except for the following: • Semicolon (;) • Comma (,) • Quote (“) • Equal (=) • Pipe (|) • Lesser than (<) • Greater than (>) • Forward slash (/) • Ampersand (&)	`$Attr1` and `$Attr2`: obtains value from `Attr1` and `Attr2` of PHONEKEY parameter.
Idle **Incoming** **Active** **Outgoing**	`Type=Function`	Call		
Active **Remote Active** **Remote Held**		Barge-in		For the soft key to appear, you must enable SCA call barge-in
Incoming **Incoming Visual** **Remote Held**		Pickup		For the soft key to appear, you must enable SCA call pickup

Table continues…

SCA Call Appearance State	Soft key setting	`Action`	`Label`	Additional parameters
Incoming **Incoming Visual**		Ignore		For the soft key to appear, you must enable **Alerting on calls** for SCA
Active		Private Hold		Private Hold is available only for Broadworks.
Idle **Incoming** **Active** **Held** **Remote Active** **Remote Held** **Conference Active**		New Call		
Active **Active PagetargetTransfer DialingConference ActiveConference Dialing**		End Call		
Active **Held**		Details		
Idle **DialtoneDialing**		Redial		
Transfer Outgoing **Transfer Consult**		Complete		
Conference Active		Add		
Conference ActiveConference Consult		Join		
Conference Active		Drop		

Table continues…

SCA Call Appearance State	Soft key setting	Action	Label	Additional parameters
Conference Consult **Conference Outgoing** **Transfer Dialing** **Transfer Consult**		Cancel		
Dialing **Transfer DialingConference Dialing**		Clear		

BLF Call Appearance State	Soft key setting	Action	Label	Additional parameters
All the Call Appearance States	`Type=Blank`	Null	Null	
Idle **Active** **Outgoing**	`Type=Dial`	Allows: • 0 to 9 • Letters (a to z) • Asterisk (*) • Pound (#)	String value. Allows any UNICODE symbol, except for the following: • Semicolon (;) • Comma (,) • Quote (“) • Equal (=) • Pipe (|) • Lesser than (<) • Greater than (>) • Forward slash (/) • Ampersand (&)	`$Attr1` and `$Attr2`: obtains value from `Attr1` and `Attr2` of PHONEKEY parameter.
Idle **Incoming** **Active** **Outgoing**	`Type=Function`	Call		
Active		Barge-in		For the soft key to appear, you must enable BLF call barge-in
Incoming **Incoming Visual**		Pickup		For the soft key to appear, you must enable BLF call pickup
Incoming **Incoming Visual**		Ignore		For the soft key to appear, you must enable **Alerting on calls** for BLF

Related links

Configuration of soft key parameter for Busy lamp field call appearance states on page 245
Configuration of soft key parameter for primary call appearance state on page 226

PHONEKEY parameter values

This section contains the full list of PHONEKEY parameter values and their definition.

The common syntax for the PHONEKEY parameter is the following:

```
SET PHONEKEY "Key=1;Type=feature;Name=autocallback"
```

where

`Type`, `Name` and `Label` can take other values. `Label` is used for localization purposes and accepts non-Latin symbols as valid values. For the full list of allowed values, refer to the table below. For additional settings of the PHONEKEY parameter and the details on its syntax, refer to the **Additional parameters** column.

Note:

The features supported only in the Broadsoft environment are marked with one asterisk (*). The features supported in both the Broadsoft and Asterisk environments are marked with double asterisk (**).

The unmarked features are supported in the Broadsoft, and Asterisk environments.

PHONEKEY setting	Allowed valuesname	Definition	Additional parameters
Feature (`Type=feature`)	callpark	Call Park*	SET PHONEKEY "Key=5;Type=feature;Name=callfwd;Label=FWD"
	callunpark	Call Unpark*	
	groupcallpark	Group Call Park*	
	callpickup	Call Pickup*	
	groupcallpickup	Group Call Pickup*	
	callwaiting	Call Waiting*	
	callfwd	Call Forward**	
	callfwdna	Call Forward No Answer**	
	callfwdbusy	Call Forward Busy**	
	dnd	Do Not Disturb**	
	autoanswer	Auto Answer**	
	bwanywhere	Broadworks Anywhere*	

Table continues…

PHONEKEY setting	Allowed values`name`	Definition	Additional parameters
	bwmobility	Broadworks Mobility*	
	callretrieve	Call Retrieve*	
	simultaneous	Simultaneous Ring Personal*	
	bwguestlogin	Flexible Seating*	
	blf	Busy Lamp Field**	Specify the following: • `Attr1` : user ID or BLF ID • `Attr2` : destination extension `SET PHONEKEY "Key=1;Type=feature;Name=blf;attr1=blf2065852005;attr2=88053"` The PHONEKEY syntax depends on the BLF mode. If `Attr2` is defined for BLF, and `label` is not defined, the `Attr2` is used as the default label for BLF. If `Attr1` is defined for BLF, `Attr2` and `label` are not defined, the `Attr1` is used as the default label for BLF. If `Attr2` is a null value, then `Attr1` is the destination extension. **Note:** The number of configured BLF lines must not exceed the total number of the phone lines. Both `Attr1` and `Attr2` are used only in the RingCentral environment.
	blfpark	Shared Parking	Specify the shared phone extension as `attr1`: `SET PHONEKEY "Key=5;Type=feature;Name=blfpark;attr1=SP1"`
	bscc	Broadworks Call Center* Activate the view providing Call Center features	

Table continues…

PHONEKEY setting	Allowed valuesname	Definition	Additional parameters
	bw-cc-dispcode	Disposition Code* Activate the view to select a disposition code	
	bw-cc-escal	Emergency escalation* Activate the view to involve a supervisor in a call or just call a supervisor	
	bw-cc-cot	Customer Originated Trace* Invoke Customer Originated Trace	
	bwcc-acd-available	Broadworks Call Center* Set the agent's state to Available	
	bwcc-acd-unavailable	Broadworks Call Center* Set the agent's state to Unavailable, and also activate the view to choose an unavailable code	
	bwcc-acd-wrap-up	Broadworks Call Center* Set the agent's state to Wrap-Up	
	bwcc-acd-sign-in	Broadworks Call Center* Set the agent's state to Sign-In	
	bwcc-acd-sign-out	Broadworks Call Center* Set the agent's state to Sign-Out	

Table continues…

PHONEKEY setting	Allowed values`name`	Definition	Additional parameters
	SendMpage	Send multicast page	`attr1` is a mandatory parameter, which is a multicast address defined in MP_GROUPS_TO_SEND. `attr2` is a mandatory parameter, which is a port defined in MP_GROUPS_TO_SEND: `SET PHONEKEY "Key=8;Type=Feature;name=SendMpage;attr1=239.0.0.0;attr2=1208;Label=Sales"`
Application (`Type=application`)	lock	Lock the phone	SET PHONEKEY "Key=1;Type=Application;Name=contacts;Label=Contacts"
	logout	User logout	
	calendar	Access Calendar	
	screensaver	Activate the screen saver	
	guestlogin	Guest Login	
	wmlbrowser	WML browser	
	recents	Access Recents	
	contacts	Access Contacts	
Line (`Type=line`)	primary	Primary line appearance	Specify the required line appearance index as `attr1`: `SET PHONEKEY "Key=1;Type=line;Name=primary;attr1=1"`
	sca	Shared Call Appearance	Specify the required shared line appearance index as `attr1` and shared line extension as `attr2`: `SET PHONEKEY "Key=1;Type=line;Name=sca;attr1=1;attr2=6837"`

Table continues…

PHONEKEY setting	Allowed valuesname	Definition	Additional parameters
Autodial (`Type=autodial`)	autodial	Automatic dialing of a phone number	Specify the required phone extension as `attr1`: `SET PHONEKEY "Key=1;Type=autodial;Name=autodial;attr1=6837"` **Note:** In Open SIP mode, automatic dialing can be configured only by setting the PHONEKEY parameter. Enhanced local dialing rules can be applied to automatic dialing by setting the ELD_SYSNUM parameter in the `46xxsettings.txt` file. To disable enhanced local dialing rules, set ELD_SYSNUM to 0.

Related links

BLF configuration modes on page 556
Setting Pre-configuration of keys on page 207
Pre-configuration of keys on page 221
Pre-configuration of keys parameter on page 221

BLF configuration modes

There are two configuration modes for Busy Lamp Field and they depend on the server envitonment.

BLF configuration through BLF_LIST_URI

In this mode, the BLF_LIST_URI parameter value is provided in the `46xxsettings.txt` file or in the web interface of the Administration menu. There are no BLF PHONEKEY values configured in the `46xxsettings.txt` file, because the phone takes BLFs from the BLF_LIST_URI.

There are two configuration parameters that determine how the BLFs detected from the list URI are placed on the phone, BLF_LIST_PREFERRED_START_LOCATION and BLF_LIST_LINEKEY_LOCATION_FORCED.

BLF_LIST_PREFERRED_START_LOCATION parameter controls where the phone places detected BLFs on the home screen. The phone detects the BLFs from the BLF_LIST_URI. This parameter provides the starting location from which the phone places detected BLFs.

BLF_LIST_LINEKEY_LOCATION_FORCED controls whether user can modify BLF line keys. When this parameter value is set to forced, the phone places detected BLFs sequentially in empty locations, starting from the point set in BLF_LIST_PREFERRED_START_LOCATION and users cannot change, move, delete or label them.

. When BLF_LIST_LINEKEY_LOCATION_FORCED is set to non-forced, the phone sequentially places all BLFs detected from the server that are not already present on the phone. Users can change, move, delete or relabel them.

It is recommended to set BLF BLF_LIST_LINEKEY_LOCATION_FORCED value to Forced in this mode so that the user cannot modify the BLF line keys.

Note:

This mode is supported in the Broadworks and Asterisk environments.

BLF configuration through PHONEKEY

In this mode, the BLF_LIST_URI parameter value is not provided in the `46xxsettings.txt` file or in the web interface of the Administration menu, the BLF phone key value must specify a UserID as `attr1` and a phone number extension as `attr2`. The phone uses `attr1` for subscriptions and `attr2` for calls.

In RingCentral environment the BLF PHONEKEY value must specify a particular BLF ID or User ID as `attr1` and phone extension as `attr2`. You need to specify both `attr1` and `attr2` for RingCentral.

For example:

```
SET PHONEKEY
"Key=1;Type=feature;Name=blf;attr1=1234@domain.name;attr2=88053;Label=1234_BLF"
```

For example:

```
SET PHONEKEY
"Key=1;Type=feature;Name=blf;attr1=1234@domain.name;attr2=1234;Label=1234_BLF"
```

for both attributes.

```
SET PHONEKEY "Key=1;Type=feature;Name=blf;attr1=1234;Label=1234_BLF"
```

for one attribute.

Note:

This mode is supported in the Asterisk, and RingCentral environments.

BLF Line type characteristics

A unique BLF line only shows once on the phone screen. `attr1` determines the uniqueness of a BLF. If there are multiple phonekeys representing the same BLF line, the phone uses the first one on the list. For example:

```
SET
PHONEKEY"Key=1;Type=feature;Name=blf;attr1=1234@domain.name;attr2=88053;Label=1234_BLF
```

```
SET PHONEKEY
"Key=2;Type=feature;Name=blf;attr1=1234@domain.name;attr2=88053;Label=1234_BLF"
```

In this case, the phone ignores Key 2.

Related links

PHONEKEY parameter values on page 552

Nesting of WML elements

The following table gives an overview of WML elements and shows which elements can be contained, or nested, within other elements:

1	2	3	4	5	6	7	8	9
wml	card	do	go	postfield				
				setvar				
			prev	setvar				
			refresh	setvar				
			noop					
		onevent	go	postfield				
				setvar				
			noop					
			prev	setvar				
			refresh	setvar				
		p	a	br				
				img				
			anchor	br				
				go	postfield			
					setvar			
				img				
				prev	setvar			
				refresh	setvar			
			br					
			do	go	postfield			
					setvar			
				prev	setvar			
				refresh	setvar			
				noop				
			img					
			input					
			select	optgroup	option	onevent	go	postfield
								setvar
							noop	
							prev	setvar
							refresh	setvar

Table continues…

1	2	3	4	5	6	7	8	9
				option	onevent	go	postfield	
							setvar	
						noop		
						prev	setvar	
						refresh	setvar	
		timer						
	head	meta						
	template	do	go	postfield				
				setvar				
			prev	setvar				
			refresh	setvar				
			noop					
		onevent	go	postfield				
				setvar				
			noop					
			prev	setvar				
			refresh	setvar				

Related links

WML syntax specifications for Avaya J100 Series IP Phones on page 559
WML browser on page 340
WML syntax specifications for Avaya J100 Series IP Phones on page 559

WML syntax specifications for Avaya J100 Series IP Phones

General WML syntax specifications

The following table shows WML syntax requirements supported by Avaya J100 Series IP Phones and exceptions to them:

Specification	External standard reference	Exception
Support for HTTP and HTTPS to obtain files specified by URLs and negotiate to SSL 3.0	N/A	No

Table continues…

Specification	External standard reference	Exception

WML 1.3 support	Wireless Application Protocol, Wireless Markup Language Specification, Version 1.3, WAP-191-WML	The following are the groups of 1.3 elements are their attributes which will be ignored by the Avaya J100 Series IP Phones WML browser:
		• access control element: `<access>`
		• text formatting elements: `<b>`, `<big>`, `<em>`, `<i>`, `<pre>`, `<small>`, `<strong>`, `<u>`
		• fieldset element: `<fieldset>`
		• table elements: `<table>`, `<td>`, `<tr>`

A `<wml>` element can contain files up to 1 MB. All data exceeding this limit will be discarded.	N/A	No
Support for WML encoded by the UFT-8 encoding of Unicode	The Unicode Standard, Version 5.0, Fifth Edition	The UTF-16 encoding of Unicode is not supported.
Support for the following WML variables: • `IPADD` • `MACADDR` • `MODEL` • `PHONEXT`	N/A	Changing the value of these variables via a `<setvar>` element is not allowed.
A History Stack can store URLs and ID attributes for up to 100 cards. If the History Stack is full, the oldest entry will be deleted before a new entry is added.	N/A	No

Table continues…

Specification	External standard reference	Exception
Error messages are created in the following cases: • a WML file cannot be obtained. • a WML file is encoded in a non-supported character encoding. • A card cannot be rendered. • A WML file is too large. Avaya J100 Series IP Phones display the "`Page cannot be rendered`" notification.	N/A	Any undefined 4xx response code is treated as 400 (Bad Request). Any undefined 5xx response code is treated as 500 (Internal Server Error).

WML elements in Avaya J100 Series IP Phones

The following table shows WML elements supported by the Avaya J100 Series IP Phones WML browser, their attributes, values, and description:

Element name	Attributes and values	Description
`<wml>`	`style`: specifies CSS properties. If not defined specifically, all child elements inherit this element. For more information about this attribute syntax and values, see Cascading Style Sheet support on page 573.	A core WML element. Inherits values from the Cascading Style Sheets (CSS) color properties of the default text.
`<head>`	N/A	A core WML element. Contains only a `<meta>` element. This element is not visually rendered on Avaya J100 Series IP Phones.
`<meta>`	The following attributes are supported: • `content`: specifies a description of the `name` attribute. • `name`: specifies the name portion of `content` and `name` values.	A core WML element. It is not visually rendered. The `name` attribute can be only specified as `title`, and its value is rendered as the title on the Title line of a WML browser.

Table continues…

Element name	Attributes and values	Description
<card>	The following attributes are supported: • newcontext The following values are allowed: - true: all variable bindings and the History Stack will be cleared - false (default) • onenterbackward: specifies a URI to be processed if the card is rendered as the result of a prev task or as the result of a Back operation on the History Stack. • onenterforward: specifies a URI to be processed if the card is rendered as the result of a go task or as the result of a Forward operation on the History Stack. • ontimer: specifies a URI to be processed when the timer expires. • style • title: specifies a card title. The default value is New card.	A core WML element. Equivalent to an HTML page element.
<template>	The following attributes are supported: • onenterbackward • onenterforward • ontimer • style	This element is used to apply do and onevent elements to all cards in a deck. The event type set as an attribute has a higher priority than the event type set in a <onevent> element. However, if event attribute is not set in a <template> element, it is inherited from an <onevent> element.
 	Only style attribute is supported for this element.	A WML element which defines a line break.

Table continues…

Element name	Attributes and values	Description
<p>	The following attributes are supported: • align: specifies how the content is aligned. The set alignment applies to all content except for <input> elements which always align left. The following values are allowed: - left (default) - right - center • mode: specifies whether the text within the paragraph can rendered on multiple lines. The following values are allowed: - wrap (default) - nowrap • style	A WML element which defines a paragraph of the text which is rendered in a new line. This element can contain the following text elements: • <p> • <a> • <anchor> • <option>
<a>	The following attributes are supported: • accesskey: specifies a dial pad key used to activate the element. If this attribute is specified, any text contained within the <a> element will not be rendered. The value is one character which can be digits 0 – 9, '*' or '#' • href: specifies the URI to be processed when the element is activated. For more information about this attribute values, see URI support on page 572. • style • title: specified a title for the element.	This element provides a simpler alternative to an anchor element with an embedded <go> element.

Table continues…

Element name	Attributes and values	Description
<anchor>	The following attributes are supported: • accesskey The value is one character which can be digits 0 – 9, '*' or '#' • style • title	Enables navigation between WML cards of the same deck or a different one.
<img>	The following attributes are supported: • alt: specifies alternative text to display if the image cannot be rendered. The default value is Image not rendered. • hspace: specifies space to the left and to the right of the image, either in pixels (n) or as a percentage of the phone screen width (n%). The default value is 0 pixels. • src: specifies the URL from which the image is obtained. • style • vspace: specifies the space above and below the image either in pixels (n) or as a percentage of the scroll panel height (n%). The default value is 0 pixels.	A WML element used to include an image in a WML card.

Table continues…

Element name	Attributes and values	Description
<do>	The following attributes are supported: • type: a mandatory attribute. Specifies the type of the <do> element. The following values are allowed: - accept - delete - help - options - prev - reset - unknown • label: specifies a label for the <do> element. If this attribute is not specified, the default value of the label attribute is based on the type attribute value, i.e., Accept, Delete, Help, Options, Back (prev), Refresh (Reset), Unknown. • name: specifies a name for the <do> element. • style	A WML element used to associate a UI element to a certain task. The <do> element can be used to specify soft keys additional to default soft keys. **Note:** In Input mode, the **Edit** soft key is added to empty locations. If no <do> elements are specified, the default soft keys are rendered (the order of list items corresponds to four soft key labels from left to right): • empty • **Home** • **Refresh** • **Exit** If one <do> element is specified, it is displayed on the leftmost soft key and the default soft keys are shifted to the right: • first <do> • **Home** • **Refresh** • **Exit** If two <do> elements are specified, they are displayed as follows: (Page 1 soft keys) • first <do> • second <do> • empty • **More** (Page 2 soft keys) • **Home** • **Refresh** • **Exit** • **More**

Table continues…

Element name	Attributes and values	Description
		If three <do> elements are specified, they are displayed as follows: (Page 1 soft keys) • first <do> • second <do> • third <do> • **More** (Page 2 soft keys) • **Home** • **Refresh** • **Exit** • **More** If four <do> elements are specified, they are displayed as follows: (Page 1 soft keys) • first <do> • second <do> • third <do> • **More** (Page 2 soft keys) • fourth <do> • **Home** • **Refresh** • **More** (Page 3 soft keys) • empty • empty • **Exit** • **More** If five <do> elements are specified, they are displayed as follows:

Table continues…

Element name	Attributes and values	Description
		(Page 1 soft keys) • first `<do>` • second `<do>` • third `<do>` • **More** (Page 2 soft keys) • fourth `<do>` • fifth `<do>` • empty • **More** (Page 3 soft keys) • **Home** • **Refresh** • **Exit** • **More**

Table continues…

Element name	Attributes and values	Description
<onevent>	Only type attribute is supported for this element. It specifies the type of the event. The following values are allowed: • onenterbackward: occurs when a <prev> task is activated or when a Back operation is invoked on the History Stack. • onenterforward: occurs when a <go> task is activated or when a Forward operation is invoked on the History Stack. • onpick: occurs when an <option> element is selected or deselected. • ontimer: occurs when a timer expires. **Note:** onenterbackward, onenterforward and ontimer attribute values are allowed when the <onevent> element is included into a <template> or a <card> element.	A WML element used to handle events. The Avaya J100 Series IP Phones WML browser supports four standard types of WML events. This element is not visually rendered.
<postfield>	The following attributes are supported: • name • value	A WML element used to send variables values to the server. The method used to obtain a deck is defined by method in a <go> element. This element is not visually rendered.

Table continues…

Element name	Attributes and values	Description
<go>	The following attributes are supported: • href • method: specifies an HTTP method used to obtain a deck. The following values are allowed: - post: the request data is appended to the URL. - get (default): the request data is sent in the body of the request. • sendreferer: if set to true, the URL of the current deck is included in the HTTP request in a Referer header. The allowed values are the following: - true - false (default)	A task element enclosed in the <do> element. This element is not visually rendered.
<noop>	N/A	When the <noop> element is activated, no task is performed. This element is not visually rendered.
<prev>	N/A	When the <prev> element is activated, a Back operation is invoked. This element is not visually rendered.
<refresh>	N/A	When the <refresh> element is activated, the card that contains this element is redownloaded and rerendered. The History Stack is not changed when a card is refreshed. This element is not visually rendered.

Table continues…

Element name	Attributes and values	Description
<input>	The following attributes are supported: • emptyok: specifies whether the <input> field can be empty. The following values are supported: - true (default) - false • format: specifies the data format for the input field. The following values are allowed: - N: a numeric character - M (default): any character - m: any character - *f: any number of characters of the type specified by f, where f is one of the character types specified above - nf: n characters of the type specified by f, where n is an integer from 1 to 9, and f is one of the character types specified above • <inputformat>: specifies the initial text entry mode for the input field. The following values are allowed: - alpha: sets the initial text entry mode to “abc” ALPHA: sets the text entry mode to “ABC” Alpha: sets the text entry mode to “Abc” Num: sets the text entry mode to “123” • ivalue: specifies the text rendered in the input field when the input element is not activated, if the value bound to the variable specified by the name attribute is null. If the value bound to the variable specified by the name attribute is not	A WML element used to obtain alphanumeric data from users. Input field is also associated with a variable which stores entered data.

Table continues…

Element name	Attributes and values	Description
	null, that value is displayed when the <input> element is not activated. • maxlength: specifies the maximum number of characters that can be entered in the field. The default value is 200. • name: specifies the name of the variable that will be bound to the input string. • onsubmit: specifies an absolute or a relative URL. • style • title • type: specifies the type of the input field. The following values are allowed: - text - password • value: specifies the default value of the variable specified by the name attribute.	
<optgroup>	Only style attribute is supported for this element.	A WML element used to group different options together in a list. This element is not visually rendered.
<option>	The following attributes are supported: • onpick: specifies the URI processed if the element is activated. This attribute has a higher priority than the type set in a <onevent> element. • style • title • value: specifies the value bound to the variable specified by the name attribute of the <select> element that contains the <option> element.	A WML element used to specify an item of a selection list.

Table continues…

Element name	Attributes and values	Description
<select>	The following attributes are supported: • iname: specifies the name of the variable that is assigned to the value of the index result. The index result is the position in the list of the selected item. • ivalue: specifies the pre-selected <option> element. • multiple: specifies whether multiple items can be selected. The following values are allowed: - true - false (default) • name: specifies the name of the variable to which the value of the selected option is bound. • style • value: specifies the default value of the variable defined by the name attribute.	A data collection element used to declare variables. This element is not visually rendered.
<setvar>	The following attributes are supported: • name • value	A WML element used to declare variables. This element is not visually rendered.
<timer>	The following attributes are supported: • name • value	Declares a timer in a WML card. This element is not visually rendered.

Related links

WML browser on page 340
Nesting of WML elements on page 558

URI support

URI support is provided in a Avaya J100 Series IP Phones WML browser.

When an element containing an href attribute with a value that begins with an HTTP or HTTPS scheme is activated, it is processed as defined in the standard WML 1.3 specification.

The following are other URI schemes supported by Avaya J100 Series IP Phones:

- When an element containing a href attribute with a wtai://wp/mc;number;name! result URI value is activated, a phone call is initiated to the specified phone extension.

- When an element containing a `href` attribute with a `wtai://wp/ap;number;name!result URI` value is activated, the phone displays the Contacts Edit screen with the name value in the **Name** field and the number value in the **Number** field.

Cascading Style Sheet support

Cascading Style Sheets (CSS) specify how certain properties of an element content are rendered. Inheritance rules allow a `style` attribute to be specified for one parent element instead of specifying it for each element in the hierarchy.

A `style` attribute can be defined in the following elements: `<wml>`, `<card>`, `<p>`, `<anchor>`, `<img>`, `<option>`, `<a>`, `<input>`, `<br>`, `<optgroup>`, and `<template>`.

If not defined specifically, a `style` attribute value is applied to the element which contains this attribute and all its child elements.

Attribute syntax

Values of the `style` attribute have the following syntax:

```
property:value
```

The default values for a `style` attribute are `color:black` and `background-color:white`.

Allowed values are the following:

- color name: `black`, `blue`, `yellow`, etc.
- hex value of an RGB color, for example, `#FF0077`

Multiple properties must be separated by a semicolon:

```
<p style="color:blue; background-color:yellow">paragraph text</p>
```

Appendix B: Public CA Certificates

Public CA Certificates

As part of DES implementation, phone has inbuilt 56 Public CA certificates. The list of Public CA certificates are:

Certificate name	Issued by	Type	Key size	Sig alg	Serial number	Expires	Fingerprint (SHA-256)
Actalis Authentication Root CA	Actalis Authentication Root CA	RSA	4096 bits	SHA-256	57 0A 11 97 42 C4 E3 CC	9/22/2030 11:22	55 92 60 84 EC 96 3A 64 B9 6E 2A BE 01 CE 0B A8 6A 64 FB FE BC C7 AA B5 AF C1 55 B3 7F D7 60 66
Baltimore CyberTrust Root	Baltimore CyberTrust Root	RSA	2048 bits	SHA-1	02 00 00 B9	5/12/2025 7:59	D4 DE 20 D0 5E 66 FC 53 FE 1A 50 88 2C 78 DB 28 52 CA E4 74
Buypass Class 2 Root CA	Buypass Class 2 Root CA	RSA	4096 bits	SHA-256	2	10/26/2040 8:38	9A 11 40 25 19 7C 5B B9 5D 94 E6 3D 55 CD 43 79 08 47 B6 46 B2 3C DF 11 AD A4 A0 0E FF 15 FB 48
Buypass Class 3 Root CA	Buypass Class 3 Root CA	RSA	4096 bits	SHA-256	2	10/26/2040 8:28	ED F7 EB BC A2 7A 2A 38 4D 38 7B 7D 40 10 C6 66 E2 ED B4 84 3E 4C 29 B4 AE 1D 5B 93 32 E6 B2 4D
Cert Sign Root CA G2	Cert Sign Root CA G2	RSA	4096 bits	SHA-256	11 00 34 b6 4e c6 36 2d 36	2/6/2042 9:27	65 7C FE 2F A7 3F AA 38 46 25 71 F3 32 A2 36 3A 46 FC E7 02 09 51 71 07 02 CD FB B6 EE DA 33 05

Table continues…

Certificate name	Issued by	Type	Key size	Sig alg	Serial number	Expires	Fingerprint (SHA-256)
Certum Trusted Network CA	Certum Trusted Network CA	RSA	2048 bits	SHA-1	04 44 C0	12/31/2029 8:07	07 E0 32 E0 20 B7 2C 3F 19 2F 06 28 A2 59 3A 19 A7 0F 06 9E
Certum Trusted Network CA 2	Certum Trusted Network CA 2	RSA	4096 bits	SHA-512	21 D6 D0 4A 4F 25 0F C9 32 37 FC AA 5E 12 8D E9	10/6/2046 8:39	B6 76 F2 ED DA E8 77 5C D3 6C B0 F6 3C D1 D4 60 39 61 F4 9E 62 65 BA 01 3A 2F 03 07 B6 D0 B8 04
COMODO ECC Certification Authority	COMODO ECC Certification Authority	ECDSA	384 bits	SHA-384	1F 47 AF AA 62 00 70 50 54 4C 01 9E 9B 63 99 2A	1/18/2038 23:59	17 93 92 7A 06 14 54 97 89 AD CE 2F 8F 34 F7 F0 B6 6D 0F 3A E3 A3 B8 4D 21 EC 15 DB BA 4F AD C7
COMODO RSA Certification Authority	COMODO RSA Certification Authority	RSA	4096 bits	SHA-384	4C AA F9 CA DB 63 6F E0 1F F7 4E D8 5B 03 86 9D	1/18/2038 23:59	52 F0 E1 C4 E5 8E C6 29 29 1B 60 31 7F 07 46 71 B8 5D 7E A8 0D 5B 07 27 34 63 53 4B 32 B4 02 34
DigiCert Global Root CA	DigiCert Global Root CA	RSA	2048 bits	SHA-1	08 3B E0 56 90 42 46 B1 A1 75 6A C9 59 91 C7 4A	11/9/2031 8:00	A8 98 5D 3A 65 E5 E5 C4 B2 D7 D6 6D 40 C6 DD 2F B1 9C 54 36
DigiCert Global Root G2	DigiCert Global Root G2	RSA	2048 bits	SHA-256	03 3A F1 E6 A7 11 A9 A0 BB 28 64 B1 1D 09 FA E5	1/15/2038 12:00	CB 3C CB B7 60 31 E5 E0 13 8F 8D D3 9A 23 F9 DE 47 FF C3 5E 43 C1 14 4C EA 27 D4 6A 5A B1 CB 5F
DigiCert Global Root G3	DigiCert Global Root G3	ECDSA	384 bits	SHA-384	05 55 56 BC F2 5E A4 35 35 C3 A4 0F D5 AB 45 72	1/15/2038 12:00	31 AD 66 48 F8 10 41 38 C7 38 F3 9E A4 32 01 33 39 3E 3A 18 CC 02 29 6E F9 7C 2A C9 EF 67 31 D0

Table continues…

Certificate name	Issued by	Type	Key size	Sig alg	Serial number	Expires	Fingerprint (SHA-256)
DigiCert High Assurance EV Root CA	DigiCert Trusted Root G4	RSA	2048 bits	SHA-1	02 AC 5C 26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	11/9/2031 8:00	5F B7 EE 06 33 E2 59 DB AD 0C 4C 9A E6 D3 8F 1A 61 C7 DC 25
DigiCert Trusted Root G4	DigiCert Trusted Root G4	RSA	4096 bits	SHA-384	05 9B 1B 57 9E 8E 21 32 E2 39 07 BD A7 77 75 5C	1/15/2038 12:00	55 2F 7B DC F1 A7 AF 9E 6C E6 72 01 7F 4F 12 AB F7 72 40 C7 8E 76 1A C2 03 D1 D9 D2 0A C8 99 88
D-TRUST Root Class 3 CA 2 2009	D-TRUST Root Class 3 CA 2 2009	RSA	2048 bits	SHA-256	09 83 F3	11/5/2029 8:35	49 E7 A4 42 AC F0 EA 62 87 05 00 54 B5 25 64 B6 50 E4 F4 9E 42 E3 48 D6 AA 38 E0 39 E9 57 B1 C1
D-TRUST Root Class 3 CA 2 EV 2009	D-TRUST Root Class 3 CA 2 EV 2009	RSA	2048 bits	SHA-256	09 83 F4	11/5/2029 8:50	EE C5 49 6B 98 8C E9 86 25 B9 34 09 2E EC 29 08 BE D0 B0 F3 16 C2 D4 73 0C 84 EA F1 F3 D3 48 81
emSign ECC Root CA-C3	emSign ECC Root CA-C3	ECDSA	384 bits	SHA-384	7b 71 b6 82 56 b8 12 7c 9c a8	2/18/2043 18:30	BC 4D 80 9B 15 18 9D 78 DB 3E 1D 8C F4 F9 72 6A 79 5D A1 64 3C A5 F1 35 8E 1D DB 0E DC 0D 7E B3
emSign ECC Root CA - G3	emSign ECC Root CA - G3	ECDSA	384 bits	SHA-384	3c f6 07 a9 68 70 0e da 8b 84	2/18/2043 18:30	86 A1 EC BA 08 9C 4A 8D 3B BE 27 34 C6 12 BA 34 1D 81 3E 04 3C F9 E8 A8 62 CD 5C 57 A3 6B BE 6B
emSign Root CA - C1	emSign Root CA - C1	RSA	2048	SHA-256	ae cf 00 ba c4 cf 32 f8 43 b2	2/18/2043 18:30	12 56 09 AA 30 1D A0 A2 49 B9 7A 82 39 CB 6A 34 21 6F 44 DC AC 9F 39 54 B1 42 92 F2 E8 C8 60 8F

Table continues…

Certificate name	Issued by	Type	Key size	Sig alg	Serial number	Expires	Fingerprint (SHA-256)
emSign Root CA - G1	emSign Root CA - G1	RSA	2048	SHA-256	31 f5 e4 62 0c 6c 58 ed d6 d8	2/18/2043 18:30	40 F6 AF 03 46 A9 9A A1 CD 1D 55 5A 4E 9C CE 62 C7 F9 63 46 03 EE 40 66 15 83 3D C8 C8 D0 03 67
Entrust Root Certification Authority	Entrust Root Certification Authority	RSA	2048 bits	SHA-1	45 6B 50 54	11/27/2026 4:53	B3 1E B1 B7 40 E3 6C 84 02 DA DC 37 D4 4D F5 D4 67 49 52 F9
Entrust.net Certification Authority (2048)	Entrust Root Certification Authority - G2	RSA	2048 bits	SHA-1	38 63 DE F8	7/24/2029 10:15	50 30 06 09 1D 97 D4 F5 AE 39 F7 CB E7 92 7D 7D 65 2D 34 31
Entrust Root Certification Authority - EC1	Entrust Root Certification Authority - EC1	ECDSA	384 bits	SHA-384	00 A6 8B 79 29 00 00 00 00 50 D0 91 F9	12/18/2037 15:55	02 ED 0E B2 8C 14 DA 45 16 5C 56 67 91 70 0D 64 51 D7 FB 56 F0 B2 AB 1D 3B 8E B0 70 E5 6E DF F5
Entrust Root Certification Authority - G2	Entrust Root Certification Authority - G2	RSA	2048 bits	SHA-256	4A 53 8C 28	12/7/2030 17:55	43 DF 57 74 B0 3E 7F EF 5F E4 0D 93 1A 7B ED F1 BB 2E 6B 42 73 8C 4E 6D 38 41 10 3D 3A A7 F3 39
GlobalSign Root CA	GlobalSign Root CA	RSA	2048 bits	SHA-1	04 00 00 00 00 01 15 4B 5A C3 94	1/28/2028 8:00	B1 BC 96 8B D4 F4 9D 62 2A A8 9A 81 F2 15 01 52 A4 1D 82 9C
GlobalSign Root E46	GlobalSign Root E46	ECDSA	384 bits	SHA-384	11 d2 bb ba 33 6e d4 bc e6 24 68 c5 0d 84 1d 98 e8 43	3/20/2046 00:00	CB B9 C4 4D 84 B8 04 3E 10 50 EA 31 A6 9F 51 49 55 D7 BF D2 E2 C6 B4 93 01 01 9A D6 1D 9F 50 58

Table continues…

Certificate name	Issued by	Type	Key size	Sig alg	Serial number	Expires	Fingerprint (SHA-256)
GlobalSign Root R46	GlobalSign Root R46	RSA	4096 bits	SHA-384	11 d2 bb b9 d7 23 18 9e 40 5f 0a 9d 2d d0 df 25 67 d1	3/20/2046 00:00	A3 12 6D 8D 3A 11 D1 C4 85 5A 4F 80 7C BA D6 CF 91 9D 3A 5A 88 B0 3B EA 2C 63 72 D9 3C 40 C9
GlobalSign	GlobalSign	ECDSA	256 bits	SHA-256	2A 38 A4 1C 96 0A 04 DE 42 B2 28 A5 0B E8 34 98 02	1/19/2038 3:14	BE C9 49 11 C2 95 56 76 DB 6C 0A 55 09 86 D7 6E 3B A0 05 66 7C 44 2C 97 62 B4 FB B7 73 DE 22 8C
GlobalSign	GlobalSign	ECDSA	384 bits	SHA-384	60 59 49 E0 26 2E BB 55 F9 0A 77 8A 71 F9 4A D8 6C	1/19/2038 3:14	17 9F BC 14 8A 3D D0 0F D2 4E A1 34 58 CC 43 BF A7 F5 9C 81 82 D7 83 A5 13 F6 EB EC 10 0C 89 24
GlobalSign	GlobalSign	RSA	2048 bits	SHA-256	04 00 00 00 00 01 21 58 53 08 A2	3/18/2029 10:00	CB B5 22 D7 B7 F1 27 AD 6A 01 13 86 5B DF 1C D4 10 2E 7D 07 59 AF 63 5A 7C F4 72 0D C9 63 C5 3B
Go Daddy Root Certificate Authority - G2	Go Daddy Root Certificate Authority - G2	RSA	2048 bits	SHA-256	0	12/31/2037 23:59	45 14 0B 32 47 EB 9C C8 C5 B4 F0 D7 B5 30 91 F7 32 92 08 9E 6E 5A 63 E2 74 9D D3 AC A9 19 8E DA
Go Daddy Class 2 Certification Authority	Go Daddy Class 2 Certification Authority	RSA	2048 bits	SHA-1	00	6/29/2034 1:06	27 96 BA E6 3F 18 01 E2 77 26 1B A0 D7 77 70 02 8F 20 EE E4
IdenTrust Commercial Root CA 1	IdenTrust Commercial Root CA 1	RSA	4096 bits	SHA-256	0A 01 42 80 00 00 01 45 23 C8 44 B5 00 00 00 02	1/16/2034 18:12	5D 56 49 9B E4 D2 E0 8B CF CA D0 8A 3E 38 72 3D 50 50 3B DE 70 69 48 E4 2F 55 60 30 19 E5 28 AE

Table continues…

Certificate name	Issued by	Type	Key size	Sig alg	Serial number	Expires	Fingerprint (SHA-256)
ISRG Root X1	ISRG Root X1	RSA	4096 bits	SHA-256	00 82 10 CF B0 D2 40 E3 59 44 63 E0 BB 63 82 8B 00	6/4/2035 11:04	96 BC EC 06 26 49 76 F3 74 60 77 9A CF 28 C5 A7 CF E8 A3 C0 AA E1 1A 8F FC EE 05 C0 BD DF 08 C6
NetLock Arany (Class Gold) Főtanúsítvány	NetLock Arany (Class Gold) Főtanúsítvány	RSA	2048 bits	SHA-256	49 41 2C E4 00 10	12/6/2028 15:08	6C 61 DA C3 A2 DE F0 31 50 6B E0 36 D2 A6 FE 40 19 94 FB D1 3D F9 C8 D4 66 59 92 74 C4 46 EC 98
Network Solutions Certificate Authority	Network Solutions Certificate Authority	RSA	2048 bits	SHA-1	57 CB 33 6F C2 5C 16 E6 47 16 17 E3 90 31 68 E0	12/31/2029 7:59	74 F8 A3 C3 EF E7 B3 90 06 4B 83 90 3C 21 64 60 20 E5 DF CE
OISTE WISeKey Global Root GC CA	OISTE WISeKey Global Root GC CA	ECDSA	384 bits	SHA- 384	21 2a 56 0c ae da 0c ab 40 45 bf 2b a2 2d 3a ea	5/9/2042 9:58	85 60 F9 1C 36 24 DA BA 95 70 B5 FE A0 DB E3 6F F1 1A 83 23 BE 94 86 85 4F B3 F3 4A 55 71 19 8D
QuoVadis Root CA 2	QuoVadis Root CA 2	RSA	4096 bits	SHA-1	05 09	11/24/2031 2:23	CA 3A FB CF 12 40 36 4B 44 B2 16 20 88 80 48 39 19 93 7C F7
QuoVadis Root CA 3	QuoVadis Root CA 3	RSA	4096 bits	SHA-1	05 C6	11/24/2031 3:06	1F 49 14 F7 D8 74 95 1D DD AE 02 C0 BE FD 3A 2D 82 75 51 85
QuoVadis Root CA 2 G3	QuoVadis Root CA 2 G3	RSA	4096 bits	SHA-256	44 57 34 24 5B 81 89 9B 35 F2 CE B8 2B 3B 5B A7 26 F0 75 28	1/12/2042 18:59	8F E4 FB 0A F9 3A 4D 0D 67 DB 0B EB B2 3E 37 C7 1B F3 25 DC BC DD 24 0E A0 4D AF 58 B4 7E 18 40
Security Communication RootCA1	Security Communication RootCA1	RSA	2048 bits	SHA-1	00	9/30/2023 12:00	36 B1 2B 49 F9 81 9E D7 4C 9E BC 38 0F C6 56 8F 5D AC B2 F7

Table continues…

Certificate name	Issued by	Type	Key size	Sig alg	Serial number	Expires	Fingerprint (SHA-256)
Security Communication RootCA2	Security Communication RootCA2	RSA	2048 bits	SHA-256	00	5/29/2029 1:00	5F 3B 8C F2 F8 10 B3 7D 78 B4 CE EC 19 19 C3 73 34 B9 C7 74
Secure Trust CA	Secure Trust CA	RSA	2048	SHA-1	0C F0 8E 5C 08 16 A5 AD 42 7F F0 EB 27 18 59 D0	12/31/2029 3:40	87 82 C6 C3 04 35 3B CF D2 96 92 D2 59 3E 7D 44 D9 34 FF 11
Starfield Class 2 Certificate Authority	Starfield Class 2 Certificate Authority	RSA	2048 bits	SHA-1	00	6/29/2034 1:39	AD 7E 1C 28 B0 64 EF 8F 60 03 40 20 14 C3 D0 E3 37 0E B5 8A
Starfield Services Root Certificate Authority - G2	Starfield Services Root Certificate Authority - G2	RSA	2048 bits	SHA-256	0	12/31/2037 23:59	56 8D 69 05 A2 C8 87 08 A4 B3 02 51 90 ED CF ED B1 97 4A 60 6A 13 C6 E5 29 0F CB 2A E6 3E DA B5
Swisscom Root CA 2	Swisscom Root CA 2	RSA	4096 bits	SHA-256	1E 9E 28 E8 48 F2 E5 EF C3 7C 4A 1E 5A 18 67 B6	6/25/2031 7:38	F0 9B 12 2C 71 14 F4 A0 9B D4 EA 4F 4A 99 D5 58 B4 6E 4C 25 CD 81 14 0D 29 C0 56 13 91 4C 38 41
Swisscom Root EV CA 2	Swisscom Root EV CA 2	RSA	4096 bits	SHA-256	00 F2 FA 64 E2 74 63 D3 8D FD 10 1D 04 1F 76 CA 58	6/25/2031 8:45	D9 5F EA 3C A4 EE DC E7 4C D7 6E 75 FC 6D 1F F6 2C 44 1F 0F A8 BC 77 F0 34 B1 9E 5D B2 58 01 5D
SwissSign Gold CA- G2	SwissSign Gold CA- G2	RSA	4096 bits	SHA-1	00 BB 40 1C 43 F5 5E 4F B0	10/25/2036 4:30	D8 C5 38 8A B7 30 1B 1B 6E D4 7A E6 45 25 3A 6F 9F 1A 27 61
SwissSign Silver CA- G2	SwissSign Silver CA- G2	RSA	4096 bits	SHA-1	4F 1B D4 2F 54 BB 2F 4B	10/25/2036 4:32	9B AA E5 9F 56 EE 21 CB 43 5A BE 25 93 DF A7 F0 40 D1 1D CB

Table continues…

Certificate name	Issued by	Type	Key size	Sig alg	Serial number	Expires	Fingerprint (SHA-256)
T-TeleSec GlobalRoot Class 2	T-TeleSec GlobalRoot Class 2	RSA	2048 bits	SHA-256	1	10/1/2033 23:59	91 E2 F5 78 8D 58 10 EB A7 BA 58 73 7D E1 54 8A 8E CA CD 01 45 98 BC 0B 14 3E 04 1B 17 05 25 52
T-TeleSec GlobalRoot Class 3	T-TeleSec GlobalRoot Class 3	RSA	2048 bits	SHA-256	1	10/1/2033 23:59	FD 73 DA D3 1C 64 4F F1 B4 3B EF 0C CD DA 96 71 0B 9C D9 87 5E CA 7E 31 70 7A F3 E9 6D 52 2B BD
Trustwave Global Certification Authority	Trustwave Global Certification Authority	RSA	4096 bits	SHA-256	05 f7 0e 86 da 49 f3 46 35 2e ba b2	8/23/2042 19:34	97 55 20 15 F5 DD FC 3C 87 88 C0 06 94 45 55 40 88 94 45 00 84 F1 00 86 70 86 BC 1A 2B B5 8D C8
Trustwave Global ECC P256 Certification Authority	Trustwave Global ECC P256 Certification Authority	ECDSA	256 bits	SHA-256	0d 6a 5f 08 3f 28 5c 3e 51 95 df 5d	8/23/2042 19:35	94 5B BC 82 5E A5 54 F4 89 D1 FD 51 A7 3D DF 2E A6 24 AC 70 19 A0 52 05 22 5C 22 A7 8C CF A8 B4
Trustwave Global ECC P384 Certification Authority	Trustwave Global ECC P384 Certification Authority	ECDSA	384 bits	SHA-384	08 bd 85 97 6c 99 27 a4 80 68 47 3b	8/23/2042 19:36	55 90 38 59 C8 C0 C3 EB B8 75 9E CE 4E 25 57 22 5F F5 75 8B BD 38 EB D4 82 76 60 1E 1B D5 80 97
USERTrust ECC Certification Authority	USERTrust ECC Certification Authority	ECDSA	384 bits	SHA-384	5C 8B 99 C5 5A 94 C5 D2 71 56 DE CD 89 80 CC 26	1/18/2038 23:59	4F F4 60 D5 4B 9C 86 DA BF BC FC 57 12 E0 40 0D 2B ED 3F BC 4D 4F BD AA 86 E0 6A DC D2 A9 AD 7A
USERTrust RSA Certification Authority	USERTrust RSA Certification Authority	RSA	4096 bits	SHA-384	01 FD 6D 30 FC A3 CA 51 A8 1B BC 64 0E 35 03 2D	1/18/2038 23:59	E7 93 C9 B0 2F D8 AA 13 E2 1C 31 22 8A CC B0 81 19 64 3B 74 9C 89 89 64 B1 74 6D 46 C3 D4 CB D2

Related links

Certificate management on page 350

Appendix C: Network progress tones overview

The SIP-based Avaya J100 Series IP Phones provide country-specific network progress tones which are presented to the user at appropriate times. The tones are controlled by administering the COUNTRY parameter for the country in which the deskphone will operate. Each Network Progress Tone has the following six components:

- Dialtone
- Ringback
- Busy
- Congestion
- Intercept
- Public Dialtone

All countries listed in this appendix are applicable to the 96xx phones. Some of the dialtone entries have changed from previous releases to be distinctively different than the public dialtone entries.

Alphabetical country list

A:

- Abu Dhabi
- Albania
- Argentina
- Australia
- Austria

B:

- Bahrain
- Bangladesh
- Belgium
- Bolivia
- Bosnia

- Botswana
- Brunei
- Bulgaria

C:

- China (PRC)
- Colombia
- Costa Rica
- Croatia
- Cyprus

D:

- Denmark

E:

- Ecuador
- El Salvador
- Egypt

F:

- Finland
- France

G:

- Germany
- Ghana
- Greece
- Guatemala

H:

- Honduras
- Hong Kong

I:

- Iceland
- India
- Indonesia
- Ireland
- Israel

J:

- Japan

- Jordan

K:

- Kazakhstan
- Korea
- Kuwait

L:

- Lebanon
- Liechtenstein
- Luxembourg

M:

- Macedonia
- Malaysia
- Mexico
- Moldova
- Morocco
- Myanmar

N:

- Netherlands
- New Zealand
- Nicaragua
- Nigeria Norway

O:

- Oman

P:

- Pakistan
- Panama
- Paraguay
- Peru
- Philippines
- Poland
- Portugal

Q:

- Qatar

R:

- Romania
- Russia

S:

- Saudi
- Arabia
- Serbia
- Singapore
- Slovakia
- Slovenia
- Spain
- South Africa
- Sri Lanka
- Swaziland
- Sweden
- Switzerland
- Syria

T:

- Taiwan
- Tanzania
- Thailand
- Turkey

U:

- Ukraine
- United Arab Emirates
- United Kingdom
- Urugua
- USA

V:

- Venezuela
- Vietnam

Y:

- Yemen

Z:

- Zimbabwe

Index

Special Characters

_REPLACE THIS TEXT, OR DELETE THIS ENTIRE INDEXTERM ELEMENT IF YOU DO NOT NEED IT 315

Numerics

802.1X
Pass-thru mode 112
supplicant 112

A

access
enabling 116
phone administration menu 116
web interface 116, 117
access control and security
security configurations 347
Active call shortcut keys
configuration 262
overview 262
admin menu
access code 94
after log in 94
administering deskphone
setting event logging 101
Site-Specific Option Number 107
viewing parameters 108
administering phone
802.1X 112
access code 94
admin menu 94
configuring SIP settings 105
debugging 98
group identifier 101
IP configuration 95
IPv4 settings 95
phone startup 94
reset to defaults 114
resetting system values 114
restarting phone 104
update info 110, 111
administration methods 36
administrative methods
file server address 34
provisioning server 34
adminstering deskphone
Ethernet interface control 99
applications 250
assign
agent 282
supervisor 282
assigning
codec priority 155
automatic
settings update 377
software update 377
automatic failback
DHCP request 65
automatic update
phone settings 377
phone software 377
Avaya support website 386

B

backup and restore
user data 374
best practices
installing the phone 376
BLF configuration 272
modes 556
Bridged Line Appearance
configuration 326
overview 325
BroadSoft
XSI 269
Broadworks
topology 89
BroadWorks
advance call control 269
call center 282
Busy Lamp Field
Alerting 272
monitored call pickup 273
overview 271
prioritizing calls 273
button modules 16
wall mounting 30

C

Calendar
configuration 252
Calendar integration 266
call
customer originated trace 283
disposition codes 283
emergency escalation 283
escalation 283
supervisor 283
trace 283
call center
agent 282
supervisor 282

Call decline policy
incoming call 288
call forward generic
web interface configuration 289
call forward on Broadsoft
overview 290
call forwarding
generic 288
call log
encryption 256
Call recording
overview 287
capture
phone network traffic 195
centralized call logs 291
centralized personal contacts 292
certificate management
security configurations 350
changing
password 119, 120, 190
phone administrator 190
Changing protocol 97
checklist
hardware setup 24
installing the phone 39
post installation 382
software setup 24
cloud configurations
MAC address file 42
phone setup process 41
settings file 42
cloud server configuration
initial setup and connectivity 41
Codec
priority 155
collection
delete 384
edit name 384
generating PDF 384
sharing content 384
computer VLAN
full VLAN separation mode 65
no VLAN separation mode 65
configuration
Broadsoft Device Management 90
Broadsoft XSI 270
DHCP 50
Shared Call Appearance 324
Shared Lines 214
Softkey sets 209
Configuration
Avaya J100 Wireless Module 28
configuration parameters 266
Configure voicemail number 342
configuring 268
Environment Setting 87, 200
Exchange Calendar 203
configuring *(continued)*
management settings 187
pre-configuration of keys 207
settings 155
softkey 210
Configuring
certificates 196
date and time 185
IP settings 132
network 124
SIP settings 143
configuring Configuring
Background 201
Screen Saver 201
configuring Group list 255
configuring provision server
file server address 34
configuring Voicemail 342
configuring Wi-Fi network
Using phone UI 104
Contacts list 254
configuration 254
content
publishing PDF output 384
searching 384
sharing 384
sort by last updated 384
watching for updates 384
Copy phone reports to USB flash drive 338
Copying phone reports 338
countries 582
country list 582
Cross-upgrade 97
CSS support 573

D

Date 47
debugging
web interface 191
DES
mutual authentication support 34
provisioning server 34
Device Enrollment Server
disabling DES 35
Device Enrollment Service
overview 32
phone installation 33, 61
Device management 90
device upgrade
process 376
DHCP
configuration 50
Option 43 codes 53
option configuration 51
site-specific parameters 55
DHCP lease

DHCP lease *(continued)*
DHCPSTD 54
DHCP server
configuration 49, 50
DHCP server configuration 49
dial plan setting 102
Digit mapping
configuration 295
overview 292
directory
downloadable 296, 545
display
secondary 16
Display name
configuration 297
disposition code
call center 283
Distinctive Alert Waiting Tone
overview 298
Distinctive Ringing
overview 298
DNS lookup 372
document changes 13
documentation center 384
finding content 384
navigation 384
documentation portal 384
finding content 384
navigation 384
download and save the software 37
dynamic
call parking 299
paging 299

E

Ethernet interface control
Ethernet setting 99
PC Ethernet setting 99
exchange authentication
basic 81
OAuth 81
exchange credential
Microsoft® 81
expansion module
upgrade overview 381
upgrading 382
Expansion module
overview 16
external switch port
configuration 64
egress tagging 64

F

feature administration
Contacts list configuration 254
feature administration *(continued)*
Group Paging configuration 305
Push-To-Talk configuration 321
Voicemail configuration 342
Feature administration
Calendar 252
calendar configuration 81, 98, 252
contacts configuration 81
features 250
Call Park 288
call waiting 291
Recents 256
field description
Exchange Calendar 204
management settings 187
NAT settings 140
network settings 125
QoS settings 138
SIP settings 144
STUN settings 140
web server settings 142
Field description
status 121
web interface 121
field descriptionfield description
Background Image 201
Screen Saver 201
field descriptions
certificates 197
Ethernet settings 133
settings 157
field descriptions, debugging 192
file server
configuring 44
finding content on documentation center 384
FIPS
FIPS mode 349
FIPS mode
security configurations 348
Flexible Seating
overview 304

G

Generate phone report 338
Generating phone report 338
Group identifier 100
Group Paging
configuration 305
overview 305

I

identifying
device type 32
identity certificates
security configurations 351

IEEE 802.1X
overview ... 111
initial setup and connectivity
cloud server configuration ... 41
initialize
phone ... 40
IP configuring
802.1Q ... 95
DNS server ... 95
gateway ... 95
HTTP server ... 95
HTTPS server ... 95
IP configuring
Auto Provisioning ... 95
IPV4 setting ... 95
IPV6 setting ... 95
mask ... 95
phone IP address ... 95
SNTP sever ... 95
use DHCP ... 95
VLAN ID ... 95
VLAN test ... 95
IPv4 and IPv6 operation
overview ... 75
IPv4 configuration
Administration menu ... 75
web interface ... 76
IPv6 configuration
Administration menu ... 79
web interface ... 80
IPv6 operation
configuration parameters ... 77
DHCPv6 configuration ... 76
limitations ... 81

J

J100 Series IP Phone models ... 15

L

language ... 219
LDAP Directory
configuration ... 306–308
list of countries ... 582
LLDP
overview ... 57
TLV impact ... 59
transmitted LLDPDU ... 58
logging in to
web interface ... 117
logging out of
web interface ... 118

M

MAC address file
cloud configurations ... 42
maintenance
downloading software upgrades ... 38
Maintenance
contents of the settings file ... 218
Microsoft exchange
authentication ... 81
Multicast Paging
configuration
settings file parameters ... 316
web UI parameters ... 205
overview ... 315
web UI field description ... 206
My Docs ... 384

N

network
VLAN ... 61
Network progress tones ... 582

O

OCSP trust certificates
security configurations ... 352
off-hook alert ... 314
open SIP operation mode ... 86
Asterisk ... 86
Avaya Cloud Office ... 86
FreeSWITCH ... 86
generic ... 86
Metaswitch ... 86
Netsapiens ... 86
RingCentral ... 86
Open SIP operation mode
BroadSoft ... 86
Open SIP operation modeBroadSoft ... 88
Option 43 codes
DHCP ... 53
option configuration
DHCP ... 51
overview ... 314
Anywhere Mobility ... 265
Avaya J100 Series IP Phones ... 15
BroadWorks Directory ... 279
LLDP ... 57
security configurations ... 345
Simultaneous Ring Personal ... 336
visual voicemail ... 343
Overview
Bluetooth ... 18
Wi-Fi ... 18

P

parameters
- BLF ... 274
- Broadworks call center ... 284
- centralized call log ... 291
- centralized personal contacts ... 292
- long-term acoustic exposure protection ... 306
- redundancy ...
  - generic Open SIP ... 366
- UI notification ... 373

Parameters ... 343, 349
- Wi-Fi ... 540

parameters redundancy, Broadsoft ... 368
parameters redundancy, Netsapiens ... 370
password
- web interface ... 118–120

periodic check
- phone settings ... 377
- phone software ... 377
- settings update ... 377
- software update ... 377

phone
- boot-up ... 32
- configuring ... 39, 219
- debugging ... 195
- lock ... 346
- network traffic ... 195
- unlock ... 346
- wall mounting ... 28

phone configuration
- administration menu ... 93
- methods ... 93
- settings file ... 217
- web interface ... 115

phone installation ... 32, 35
phone lock
- parameters ... 346

Phone report ... 338
Phone screen width
- configuration
  - overview ... 322
  - parameters ... 322
- limitations ... 323
- phone menu ... 323

phone setup process
- cloud configurations ... 41

PHONEKEY
- values ... 552

ports
- received packets ... 69
- TCP ... 69
- transmitted packets ... 70
- UDP ... 69

Power management ... 21
pre-configuration
- fields ... 208

pre-configuration of keys
- configuration ... 221
- overview ... 221
- phonekey labels ... 223
- viewing internal parameter details ... 223

precedence
- administration methods ... 36

prerequisites
- hardware ... 35
- software ... 35

Prioritization of codecs
- configuration ... 319
- overview ... 318

process
- device upgrade ... 376

protection
- long term protection ... 305

protocols
- received packets ... 69
- transmitted packets ... 70

provisioning server ... 34
provisioning server configuration ... 45, 301, 302
- server ... 45, 301, 302

Public CA Certificates ... 574
Push
- overview ... 319
- parameters ... 320

Push-To-Talk
- configuration ... 321
- overview ... 321

R

received packets
- ports ... 69
- protocols ... 69

redundancy ... 372, 373
redundancy,
- Open SIP
  - Broadsoft ... 366, 368
  - generic ... 366
  - Netsapiens ... 366, 370

related documentation ... 384
resetting
- Phone to default ... 216

ringtone
- parameters ... 257

Ringtone
- Open SIP ... 259
- personalize ... 259

Ringtonespersonalize
- default ... 257

S

SCA
- usage, usage on the phone ... 324

screen
web interface 119
Scrolling mode
configuration 333
Limitations 333
overview 332
searching for content 384
secure installation
parameters 353
Secure mode
restrictions 350, 365
secure syslog
overview 364
parameters 364
security configuration
GDPR 361
Secure mode 361, 362
security configurations
access control and security 347
certificate management 350
FIPS mode 348
identity certificates 351
Key Usage 353
OCSP trust certificates 352
overview 345
trusted certificates 352
Selection of a higher priority line 334, 335
server configuration 44
Server-initiated Update
applying settings 113
overview 335
updating firmware 113
setting
open SIP operation mode 86
settings file
Call Forward configuration 289
cloud configurations 42
configuring 39, 219
Directory 280
dynamic park and page configuration 299
Recents configuration 256
Shared Call Appearance 327
Shared lines
limitation 332
Shared Lines 327
BCA 326
Call alerts and delayed ringing 326
overview 324
web UI field description 215
Shared Parking
configuration
settings file parameters 334
overview 333
sharing content 384
sidetone
ambience noise 263
audio
audio *(continued)*
audio *(continued)*
feedback 263
Signaling 97
configuration 98
overview 97
Signaling protocol 97
updating 97
Simultaneous Ring Personal configuration 336
SIP settings
SIP global settings 105
SIP proxy server 105
site-specific parameters
DHCP 55
SNTP parameters 47
SNTP server 47
soft key
available values 546
soft key configuration 224
BLA 235
call appearance state 224
parameters 226, 235
primary call appearance 226
SCA 235
Soft key configuration
Busy lamp field call appearance 245
parameters 245
Softkey sets
web UI field description 210
software 23
downloading and saving 37
sort documents by last updated 384
specifications
hardware 18
STUN
configuration 72
overview 71
support 386
syntax
downloadable directory 545

T

TCP ports 69
Time
SETTINGS 47
Time server setting 47
TLV impact
LLDP 59
traffic
LAN port 62
PC port 62
Transfer phone reports 337
transmitted LLDPDU
LLDP 58
transmitted packets
ports 70

transmitted packets *(continued)*
protocols 70
trusted certificates
security configurations 352

U

UDP ports 69
updating uploading
directory contacts 296
USB flash drive
parameters 338
USB Flash drive
overview 337
USB Flash Drive 337
USB Headset
overview 336
parameters 337
USB keyboard
overview 339
parameters 339
USB Stick 337
user data
backup and restore 374

V

videos 386
View field description 108
STUN server details 110
viewing
IP address 117
Viewing,
phone configuration 120
status 120
view status 120
Visual Voicemail 343
VLAN
IEEE 802.1Q 61
internal switch 62
VLAN tag 61
VLAN forwarding rules
802.1x frames 65
LLDP frames 65
spanning tree frames 65
VLAN ID
VLAN ID of zero 65
VLAN separation mode
full VLAN separation mode 63
no VLAN 63
VLAN settings
configure VLAN settings 62
VLAN tagging
automatic failback 65
voice VLAN
data VLAN 61
Voicemail
Voicemail *(continued)*
configuration 342
overview 342

W

wall mounting 28
watch list 384
web interface
debugging 192
default phone web interface 119
log out 118
log-in 117
password 118
restarting phone 216
screen layout 119
web interface Configuration
NAT 139
QoS settings 138
STUN 139
web server settings 141
wireless module 28
installation 25
without DES 35
WML browser 573
configuration 340
element nesting 558
overview 340
syntax requirements 559
URI support 572