# Installing and Administering Avaya J100 Series SIP IP Phones in Avaya Aura®

Release 4.0.14
Issue 2
November 2022

© 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.

Avaya J129 IP Phone, Avaya J159 IP Phone, Avaya J179 IP Phone, and Avaya J189 IP Phone complies with the EMC Directives.

WiFi transmitter

For Avaya J129 IP Phone, Avaya J159 IP Phone, Avaya J179 IP Phone, and Avaya J189 IP Phone

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

BT transmitter

For Avaya J159 IP Phone, Avaya J179 IP Phone, and Avaya J189 IP Phone

- 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 ..... 14
**Chapter 2: Avaya J100 Series IP Phones overview** ..... 15
J100 Series IP Phone models ..... 15
Secondary display ..... 16
Wi-Fi Module ..... 16
Hardware specifications ..... 17
Power specifications ..... 20
Supported codecs ..... 22
**Chapter 3: Initial setup and connectivity** ..... 23
Initial setup checklist ..... 23
Installing the wireless module ..... 24
Wireless Module configuration ..... 26
Wall mounting Avaya J100 Series IP Phones ..... 27
Wall mounting Avaya J100 Expansion Module ..... 29
Software installation ..... 31
Identifying the device type during phone boot-up ..... 31
Automatic phone provisioning ..... 31
Automatic phone provisioning using Device Enrollment Services ..... 32
Entering the provisioning details ..... 32
Provisioning server mutual authentication support ..... 33
Disabling DES ..... 34
Manual phone provisioning ..... 34
Hardware and software prerequisites ..... 34
Administration methods ..... 35
Diagram: Phone deployment process ..... 36
Diagram: IP phone setup ..... 37
Installation checklist without DES ..... 37
Avaya Aura® System Manager user profile worksheet ..... 38
Downloading and saving the software ..... 39
Modifying the settings file ..... 40
Phone initialization ..... 41
**Chapter 4: Servers, VLAN, and IP configuration** ..... 43
Server configuration ..... 43
Setting up a provisioning server ..... 43
Provisioning Server configuration ..... 44
DHCP server configuration ..... 46
Setting up a DHCP server ..... 46

Configuration through DHCP ..... 47
DHCP Site Specific Option ..... 47
DHCP options ..... 49
Configuration through LLDP ..... 53
LLDPDU transmitted by the phones ..... 54
TLV impact on system parameter values ..... 55
SNTP server configuration ..... 57
SNTP Parameters ..... 58
Automatic phone provisioning using Device Enrollment Services ..... 60
Virtual LAN (VLAN) ..... 60
VLAN separation ..... 61
Configuring an external switch port ..... 63
Exceptions to the VLAN forwarding rules ..... 64
Special considerations ..... 64
VLAN parameters ..... 65
TCP and UDP ports ..... 68
Received packets (destination = SIP phone) ..... 68
Transmitted packets (source = SIP phone) ..... 69
IPv4 and IPv6 ..... 70
Configuring IPv4 from the phone menu ..... 71
Configuring IPv4 from the web interface ..... 71
IPv6 configuration ..... 72
Configuring IPv6 from the phone menu ..... 74
Configuring IPv6 from the web interface ..... 75
Configuring a DHCP server in the dual and IPv6-only environments ..... 75
IPv6 limitations ..... 76
DNS resolution for SIP controller ..... 76
Microsoft® Exchange account integration ..... 79
Microsoft Exchange account integration configuration parameters ..... 80
**Chapter 5: Avaya Aura configuration for phones** ..... 84
SIP phone administration on Communication Manager ..... 84
SIP phone administration on Session Manager ..... 85
Personal Profile Manager ..... 86
Avaya Aura® Device Services ..... 86
Controllers ..... 87
Administering emergency numbers ..... 87
**Chapter 6: Phone configuration** ..... 89
Configuring the phone using Administration menu ..... 89
Accessing the Admin menu during phone startup ..... 90
Accessing the Admin menu after logging in ..... 92
Accessing the Ethernet IPv4 settings ..... 92
Signaling protocol ..... 94
Using the debug mode ..... 96

Setting the Ethernet interface control ..... 97
Group identifier ..... 98
Setting event logging ..... 99
Setting the dial plan ..... 99
Administering enhanced local dialing ..... 101
Restarting the phone ..... 104
Connecting to a Wi-Fi network ..... 104
Configuring SIP settings ..... 105
Setting Site Specific Option Number (SSON) ..... 106
Using the VIEW administrative option ..... 107
Checking the phone update status ..... 109
Checking the phone update policy ..... 109
IEEE 802.1X overview ..... 110
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 ..... 118
Logging out of the phone web interface ..... 118
Password for the phone web interface ..... 119
Changing the default phone web interface password ..... 119
Web interface screen layout ..... 120
Changing the phone web interface password ..... 120
Viewing the status of the phone configuration ..... 121
Configuring network settings ..... 124
Configuring IP settings ..... 133
Configuring QoS settings ..... 139
Configuring Web Server settings ..... 140
Configuring SIP settings ..... 142
Configuring Settings ..... 153
Configuring date and time ..... 174
Configuring management settings ..... 176
Changing the password of the phone Administrator menu ..... 179
Debugging ..... 180
Capturing the phone network traffic ..... 184
Configuring Certificates ..... 185
Configuring Environment Settings ..... 191
Configuring Background and Screen Saver of the Phone ..... 192
Configuring Calendar of the phone ..... 195
Configuring Multicast Paging ..... 197
Setting Pre-configuration of keys ..... 199
Configuring softkey sets ..... 201
Restarting your phone through web interface ..... 206

Resetting the phone to Default..... 206
Configuring the phone using the settings file..... 206
Contents of the settings file..... 207
Modifying the Settings file..... 208
Phone display language..... 209
Customization modes..... 210
Always Favorites on Button Module..... 211
Customization parameters..... 212
Pre-configuration of keys..... 212
Pre-configuration of keys parameter..... 213
Phonekey Labels..... 215
Viewing PHONEKEYLIST parameter details..... 216
Keys customization restoration..... 216
Soft key configuration..... 217
Configuration of soft key parameter for primary call appearance state..... 218
**Chapter 7: Feature and application configuration**..... 228
Application configuration..... 230
Calendar..... 230
Contacts list..... 232
Recents..... 234
Agent Greeting..... 235
Feature configuration..... 236
Automatic Callback..... 236
Active call shortcut keys..... 237
Avaya Spaces Calendar integration..... 238
Busy Indicator..... 240
Call decline policy..... 240
Call Forward..... 241
Call Pickup..... 242
Call Park..... 242
Calling party number blocking..... 243
Calling party number unblocking..... 243
Call recording..... 243
Digit mapping..... 244
Enable access to restart the phone..... 248
Extension to Cellular ..... 249
Exclusion..... 250
Feature target selection..... 250
Force HTTP/HTTPS provisioning server credentials..... 251
Guest login..... 253
Hunt Group Busy Position..... 254
Intercom..... 254
Long-term acoustic protection..... 255

Limit Number of Concurrent Calls ..... 255
LDAP Directory ..... 256
Multiple Device Access ..... 263
Multiple Level Precedence and Preemption ..... 266
Multicast Paging ..... 268
Malicious call tracing ..... 270
No Hold Conference ..... 271
Night mode ..... 271
Off-hook alert ..... 272
Presence ..... 273
Prioritization of codecs ..... 276
Priority Calling ..... 276
Push ..... 277
Ringtones ..... 279
Scrolling mode ..... 282
Send All Calls ..... 283
Service Observe ..... 284
Server-initiated update ..... 284
Selection of a higher priority line after ending a call ..... 285
Team Button ..... 286
USB Headset ..... 287
USB Flash drive ..... 288
USB keyboard ..... 290
Voicemail ..... 291
WML browser ..... 292
Whisper Page ..... 295
**Chapter 8: Avaya J100 Expansion module** ..... 296
Expansion modules ..... 296
JEM24 background and screen saver image configuration ..... 297
Import background and screen saver images of JEM24 ..... 298
JEM24 background and screen saver image configuration parameters ..... 298
Configuring JEM24 background and screen saver images by using web interface ..... 301
Avaya J100 Expansion Module upgrade ..... 302
Upgrading the expansion module ..... 302
**Chapter 9: Security** ..... 304
Security overview ..... 304
Locking and unlocking the phone ..... 305
Phone lock configuration parameter ..... 306
Access control and security ..... 307
Certificate management ..... 308
Phone identity certificates ..... 309
Multiple identity certificate configuration ..... 311
Identity certificate renewal ..... 323

Trusted certificates ... 324
OCSP trust certificates ... 325
View installed phone certificates ... 325
Key Usage check for security certificates ... 326
Certificate configuration parameters ... 326
Configuration for secure installation ... 330
FIPS mode ... 333
FIPS mode parameter ... 334
**Chapter 10: Data Privacy Controls Addendum** ... 336
Purpose ... 336
Data categories containing personal data (PD) ... 336
Personal data human access controls ... 337
Personal data programmatic or API access controls ... 337
Personal data at rest encryption controls ... 338
Personal data in transit encryption controls ... 338
Personal data retention period controls ... 339
Personal data export controls and procedures ... 339
Personal data view, modify, delete controls and procedures ... 340
Personal data pseudonymization operations statement ... 341
Data privacy and secure data processing ... 341
Secure mode ... 341
Configuring secure mode parameter ... 342
Data privacy ... 342
Secure Syslog ... 344
Secure Syslog parameters ... 344
Geographical restrictions on encryption ... 345
**Chapter 11: Failover and survivability** ... 346
Redundancy with IP phone and Avaya Aura® ... 346
Detection of loss of connection ... 346
Failover to a backup proxy ... 347
Restoring the phone to the primary proxy ... 347
Proxy determination when the phone loses connection to the primary proxy ... 348
Simultaneous registration ... 348
Limitations during failover or failback ... 348
Preserved call ... 349
Limitations of call preservation ... 349
Limitations after a successful failover ... 349
Indications of redundancy ... 351
Supported non Avaya Aura® proxies for redundancy ... 351
Parameters for redundancy provisioning ... 352
Redundancy in a non-Avaya proxy environment ... 357
**Chapter 12: Backup and restore** ... 358
User profile backup on Personal Profile Manager (PPM) ... 358

User profile parameters for backup ..... 358
**Chapter 13: Maintenance** ..... 360
Using the debug mode ..... 360
Setting event logging ..... 361
Debugging ..... 362
Debugging field descriptions ..... 362
Capturing the phone network traffic ..... 366
Phone installation - best practices ..... 367
Device upgrade process ..... 368
Server-initiated update ..... 368
Periodic check for software and settings update ..... 369
Periodic check of software and settings update configuration ..... 369
Post installation checklist ..... 373
**Chapter 14: Troubleshooting** ..... 375
Phone displays Acquiring Service screen ..... 375
SLA Mon™ agent ..... 376
Error handling and troubleshooting for certificate renewal ..... 377
**Chapter 15: Resources** ..... 378
Documentation ..... 378
Finding documents on the Avaya Support website ..... 380
Avaya Documentation Center navigation ..... 380
Viewing Avaya Mentor videos ..... 381
Support ..... 382
**Appendix A: Customizable parameters** ..... 383
List of configuration parameters ..... 383
List of Wi-Fi configuration parameters ..... 502
Soft key parameter values ..... 507
PHONEKEY parameter values ..... 510
Nesting of WML elements ..... 513
WML syntax specifications for Avaya J100 Series IP Phones ..... 515
**Appendix B: Public CA Certificates** ..... 530
**Appendix C: Network progress tones overview** ..... 538

# 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, skills, and tools:

### Knowledge

- DHCP
- SIP
- Installing and configuring Avaya Aura® components
- Installing and configuring IP Office components
- 802.1x and VLAN

### Skills

Administering and configuring:

- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Presence Services
- Avaya Aura® Session Border Controller
- IP Office
- DHCP server
- HTTP or HTTPS server
- Microsoft Exchange Server

### Tools

- Avaya Aura® System Manager
- IP Office Manager
- IP Office Web Manager

# Change history

| Issue | Date | Summary of changes |
|---|---|---|
| Release 4.0.11 | February 2022 | • Updated “Configuring servers and VLAN” chapter<br>• Updated "Security" chapter<br>• Updated “Phone configuration” chapter<br>• Updated “Feature and application configuration” chapter<br>• Updated Appendix |
| Release 4.0.12 | April 2022 | • Updated “Configuring servers and VLAN” chapter<br>• Updated “Phone configuration” chapter<br>• Updated Appendix |
| Release 4.0.13 | July 2022 | • Updated "Security" chapter<br>• Updated “Phone configuration” chapter<br>• Updated “Feature and application configuration” chapter<br>• Updated Appendix |
| Release 4.0.14 | October 2022 | • Added "Avaya J100 Expansion Module" chapter<br>• Updated “Phone configuration” chapter<br>• Updated “Feature and application configuration” chapter<br>• Updated Appendix |
| Release 4.0.14 | November 2022 | • Updated “Phone configuration” chapter<br>• Updated “Maintenance” chapter<br>• 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 Avaya Aura® and IP Office 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.

# 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 |

*Table continues…*

| Model | Display (pixels) | Display type | Call appearances |
|---|---|---|---|
| J159 | 2.8”, 320 x 240 primary display<br>2.4”, 240 x 320 secondary display | Color | 4 on the primary display<br>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<br>2.4”, 240 x 320 secondary display | Color | 10 on the primary display<br>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 | Handset adapter |
|---|---|---|---|---|
| J129 | Yes | Yes, with 20dB of gain | No | Yes |
| J139 | Yes | Yes, with 20dB of gain | Yes | Yes |
| J159 | Yes | Yes, with 20dB of gain | Yes | Yes |
| J169 | Yes | Yes, with 20dB of gain | Yes | Yes |

*Table continues…*

| Model | Wired handset (HAC) | Amplified handset mode | Wired headset | Handset adapter |
|---|---|---|---|---|
| J179 | Yes | Yes, with 20dB of gain | Yes | Yes |
| J189 | Yes | Yes, with 20dB of gain | Yes | Yes |
| JBM24 | NA | NA | NA | NA |
| JEM24 | NA | 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 Avaya 5V DC power 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 Avaya 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 Avaya 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 Avaya 5V DC power 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 |

*Table continues…*

| Phone model | Avaya standard power measurements (in Watts) | | | Energy Star (in Watts) |
|---|---|---|---|---|
| | Conservation | Typical | Maximum | Standby |
| JEM24 | 1.70 | 1.90 | 2.00 | NA |
| 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.<br>• 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.<br>• 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.<br>• 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.<br>**Note:**<br>Use Avaya 5V DC power adapter if you simultaneously connect a wireless module along with one or more button modules of any model. |

*Table continues…*

| | |
|---|---|
| J189 | • IEEE 802.3af PoE Class 2, PoE slide switch in L position with a wireless module.<br>• 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<br>• G.711µ<br>• G.729<br>• G.729a<br>• G.729ab<br>• G.726<br>• G722<br>• OPUS | • G.711a<br>• G.711µ<br>• G.729<br>• G.729a<br>• G.729ab<br>• G.726<br>• G722<br>• OPUS | • G.711a<br>• G.711µ<br>• G.729<br>• G.729a<br>• G.729ab<br>• G.726<br>• G722<br>• OPUS | • G.711a<br>• G.711µ<br>• G.729<br>• G.729a<br>• G.729ab<br>• G.726<br>• G722<br>• OPUS | • G.711a<br>• G.711µ<br>• G.729<br>• G.729a<br>• G.729ab<br>• G.726<br>• G722<br>• OPUS | • G.711a<br>• G.711µ<br>• G.729<br>• G.729a<br>• G.729ab<br>• G.726<br>• G722<br>• OPUS<br>• 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.<br><br>Avaya J100 Series IP Phones ship in a box containing an IP Phone, a handset with a cord, a dual-position phone stand, and a regulatory/safety sheet.<br><br>**Note:**<br><br>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.<br><br>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.<br><br>**Note:**<br><br>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 24 | |

*Table continues…*

| No. | Task | Reference | ✔ |
|---|---|---|---|
| 4 | Assemble the phone by connecting handset, and inserting the phone stand into the slots at the back panel of the phone. | | |
| 5 | (Optional) Attach the button module to the phone.<br>**Note:**<br>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 296 | |
| 6 | 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 31<br>Manual phone provisioning on page 34 | |
| 7 | Set up the Provisioning Server for the Manual provisioning. | Provisioning Server configuration on page 44 | |
| 8 | Connect Avaya J100 Series IP Phones to the power supply and network with the Ethernet cable. | Power specifications on page 20 | |
| 9 | Perform the phone initialization following the tasks for one of the selected methods. | Phone initialization on page 41 | |

# Installing the wireless module

## Before you begin

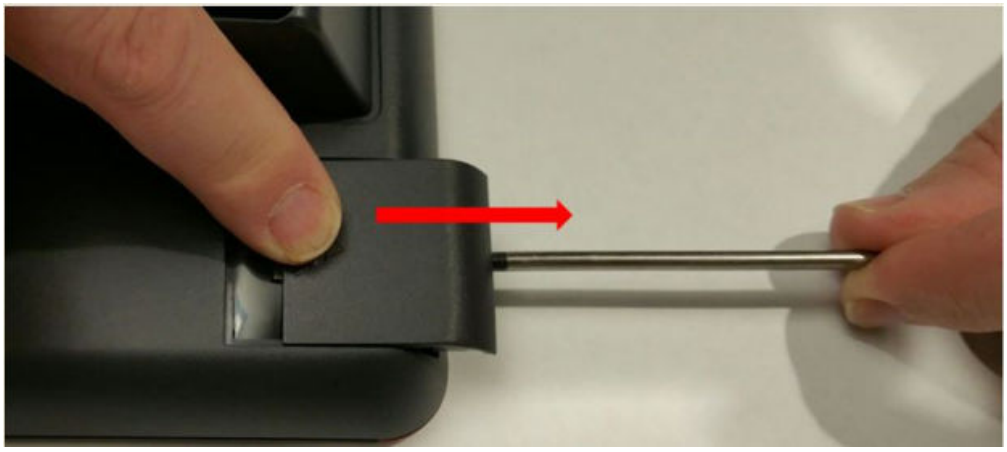
Obtain the following items:

- 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

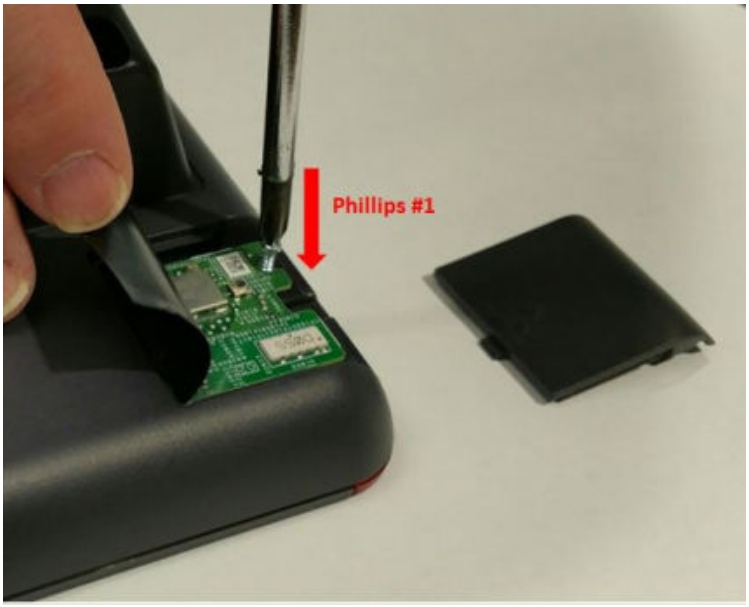
1. Insert the screw driver in the opening of the module panel to release the latch. Do not pry open the panel.

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.

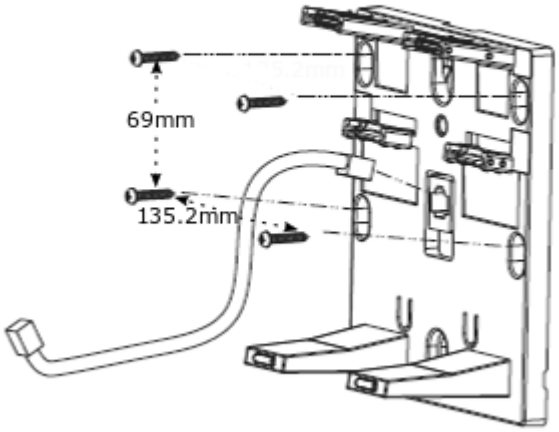
### Before you begin

Obtain the following items:

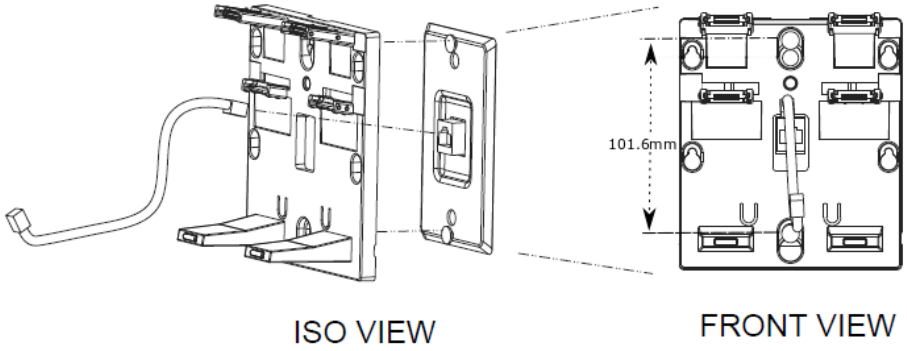
- Wall mounting kit, containing a wall mount bracket, and an Ethernet cable.
- Four #8 screws. The screws are not provided with the wall mounting kit. If the wall plate is pre-installed, you do not need the screws.

### 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.

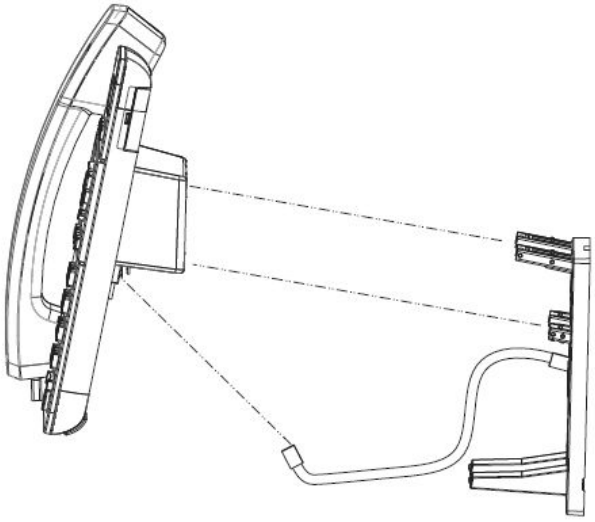



- If the wall plate is pre-installed, fit the wall mount bracket over the wall plate.




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.



**Related links**

Wall mounting Avaya J100 Expansion Module on page 29

# 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:

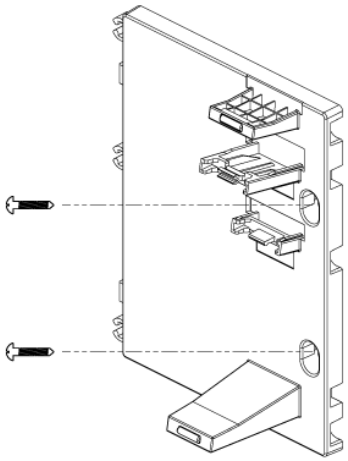
- Wall mount kit, containing a wall mount bracket.
- Two #8 screws. The screws are not provided with the wall mounting kit.
- Link for connecting expansion module for Avaya J189 IP Phone that comes along with the kit.

### Procedure

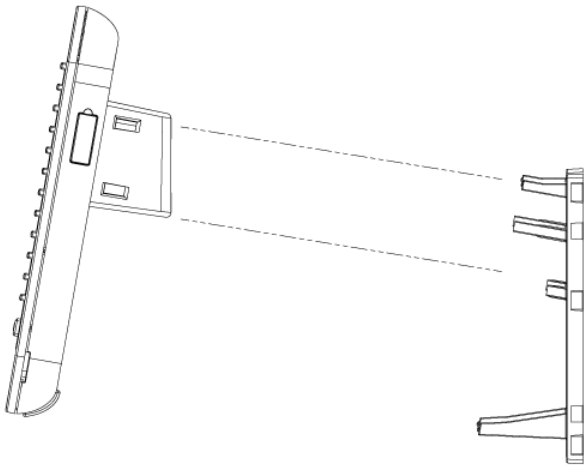
1. Remove the phone from the wall mount.
2. Place the expansion module bracket on one level to the right of the phone bracket, mark and drill holes, and then affix the #8 screws.

   **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.

**Related links**

Wall mounting Avaya J100 Series IP Phones on page 27

# 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.

For best practices of phone installation, see Phone installation - best practices on page 367.

# 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. The phone software version 4.0.3 and later supports this feature.

### Procedure

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

   The phone powers up and starts to initialize.

   The Avaya SIP phones display Avaya text for all the J100 models except Avaya J129 IP Phone. Avaya J129 IP Phones display `Starting... Avaya 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 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 phones supporting Device Enrollment Services come from the factory with a unique device certificate known to the Device Enrollment Services server. The phone software 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 32
Provisioning server mutual authentication support on page 33
Disabling DES 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, or Administration menu. If the phone fails to discover the configuration server using DHCP SSON, LLDP 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. 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 31

# 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, 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 31

## 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**

Automatic phone provisioning on page 31

# Manual phone provisioning

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

## Hardware and software prerequisites

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

### Hardware prerequisites

Ensure that the LAN:

- Uses unshielded twisted pair (UTP) Ethernet Category 5e or Category 6 cabling
- Has either of the following specifications:
  - IEEE 802.3af PoE
  - IEEE 802.3af PoE injector

**Note:**

You can also power the phone using the Avaya 5V DC power adapter. You must purchase the power adapter separately.

## Software prerequisites

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

- Avaya Aura® Session Manager 6.3.8 or later
- Avaya Aura® Communication Manager 6.3.6 or later
- Avaya Aura® System Manager 6.3.8 or later
- If applicable, Avaya Aura® Presence Services 6.2.4 or later
- If applicable, Avaya Aura® Session Border Controller 7.0 or later
- If applicable, IP Office IPO 11.0.0 or later
- A DHCP server for providing dynamic IP addresses to the Avaya J100 Series IP Phones.
- A file server, an HTTP, HTTPS, or the Avaya Aura® Utility Services for downloading the software distribution package and the settings file

IPv6 deployment requires Avaya Aura® Session Manager v7.1 or later, Avaya Aura® Communication Manager v7.1 or later, Avaya Aura® System Manager v7.1 or later, and Avaya Aura® Session Border Controller v7.1 or later. For more information about installing and configuring the components, see their respective documentation.

# Administration methods

You can use the following methods to administer the devices. The following table lists the 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 | Quality of Service | Application-specific parameters |
| DHCP | ✔ | ✔ | ✔ | — | ✔ | — | ✔ |
| LLDP | — | ✔ | ✔ | — | — | ✔ | — |
| Settings file | — | ✔ | — | ✔ | ✔ | ✔ | ✔ |
| Avaya Aura® System Manager | — | — | — | ✔ | — | — | ✔ |
| Administration menu on the phone | ✔ | ✔ | ✔ | ✔ | ✔ | — | ✔ |
| Web UI | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |

## Precedence of administration methods

Most of the parameters are configured through multiple methods. If you configure a parameter through more than one method, the device applies the settings of the method that has a higher

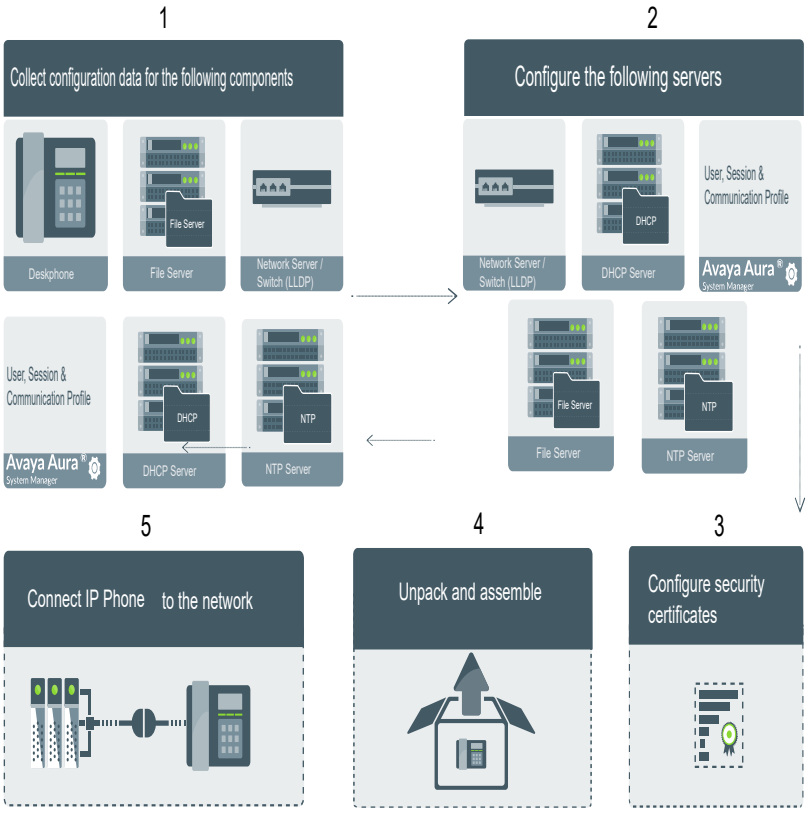
precedence. The following list shows the precedence of the methods in the highest to lowest order:

1. Administration menu on the phone. When the parameter USE_DHCP is set to 1, the phone gets the DHCP values from the DHCP rather than Administration menu of the phone.
2. Administering the phone from the web UI.
3. Avaya Aura® System Manager and IP Office.
4. `46xxsettings.txt` file
5. DHCP.
6. LLDP. There is an exception of LLDP getting a higher precedence than the `46xxsettings.txt` file and DHCP when the layer 2 parameters, such as L2QVLAN, L2Q, L2QAUD, L2QVID, L2QSIG, DSCPAUD, DSCPSIG, and PHY2VLAN are set through LLDP.

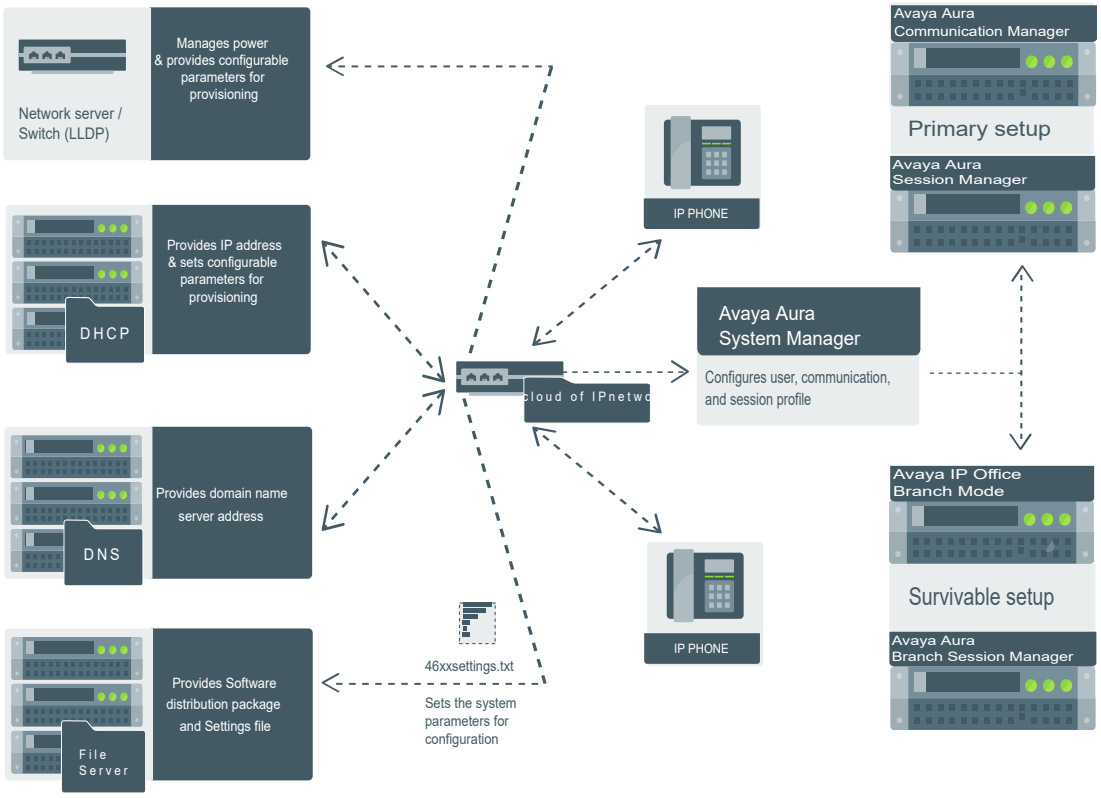
**Note:**

When parameters of the `46xxsettings.txt` file are removed, or are not used, they reset to their default value.

## Diagram: Phone deployment process



# Diagram: IP phone setup




# Installation checklist without DES

Use this checklist to gather, record, and verify the information during the installation.

| No. | Task | Reference | ✔ |
|---|---|---|---|
| 1 | Check the prerequisites. | See Hardware and software prerequisites on page 34 for more information. | |
| 2 | Configure system manager user profile. | See Avaya Aura System Manager user profile worksheet on page 38 for more information. | |
| 3 | Configure the servers. | See Server configuration on page 43 for more information. | |
| 5 | Configure LLDP. | See Configuration through LLDP on page 53 for more information. | |
| 6 | Configure VLAN. | See Virtual LAN (VLAN) on page 60 for more information. | |
| 7 | Install the phone. | See Phone initialization on page 41 for more information. | |

# Avaya Aura® System Manager user profile worksheet

Populate the values in the corresponding fields before stating the installation process of the phone.

| Data for | Field | Value | Notes |
|---|---|---|---|
| **System Manager User Profile** | | | |
| **Identity tab** | | | |
| | Login Name | | |
| | Localized Display Name | | |
| | Endpoint Display Name | | |
| | Language Preference | | |
| | Time Zone | | |
| **Presence Profile** | | | |
| | System | | |
| | IM Gateway SIP Entity | | |
| | Publish Presence with AES collector | | |
| **Communication Profile tab** | | | |
| **Communication Profile section** | | | |
| | Communication Profile Password | | |
| **Session Manager Profile section** | | | |
| | Primary Session manager | | |
| | Secondary Session Manager | | |
| | Survivability Server | | |
| **CM Endpoint Profile section** | | | |
| | System | | |
| | Profile Type | | |
| | Use Existing Endpoints | | |
| | Extension | | |
| | Endpoint Template | | |
| | Voice Mail Number | | |
| | Presence server | | |

*Table continues…*

| Data for | Field | Value | Notes |
|---|---|---|---|
| | Conference server | | |
| **Messaging Profile section** | | | Optional |
| | System | | |
| | Mailbox Number | | |
| | Template | | |
| | Password | | |
| **SIP settings** | | | For registering phones. |
| | SIP controller list | | |
| | SIP domain | | |
| **File server address** | | | To download the software distribution package and the `Settings` file. |
| | HTTP server or TLS server | | Set the appropriate file server address in the `46xxsettings.txt` file, LLDP and DHCP. |

**Note:**

For information about IP Office preinstallation data gathering, see *Avaya IP Office Platform 10.0 SIP Telephone Installation Notes*.

# 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.

# Phone initialization

### Before you begin

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, such as, 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, 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.

Use the Post installation checklist to ensure the phone is installed and running correctly.

**Related links**

Post installation checklist on page 373

# 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 47

## 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` file.
3. Extract the distribution package, and save the extracted files and the `46xxsettings.txt` file on the provisioning server.

# Provisioning Server configuration

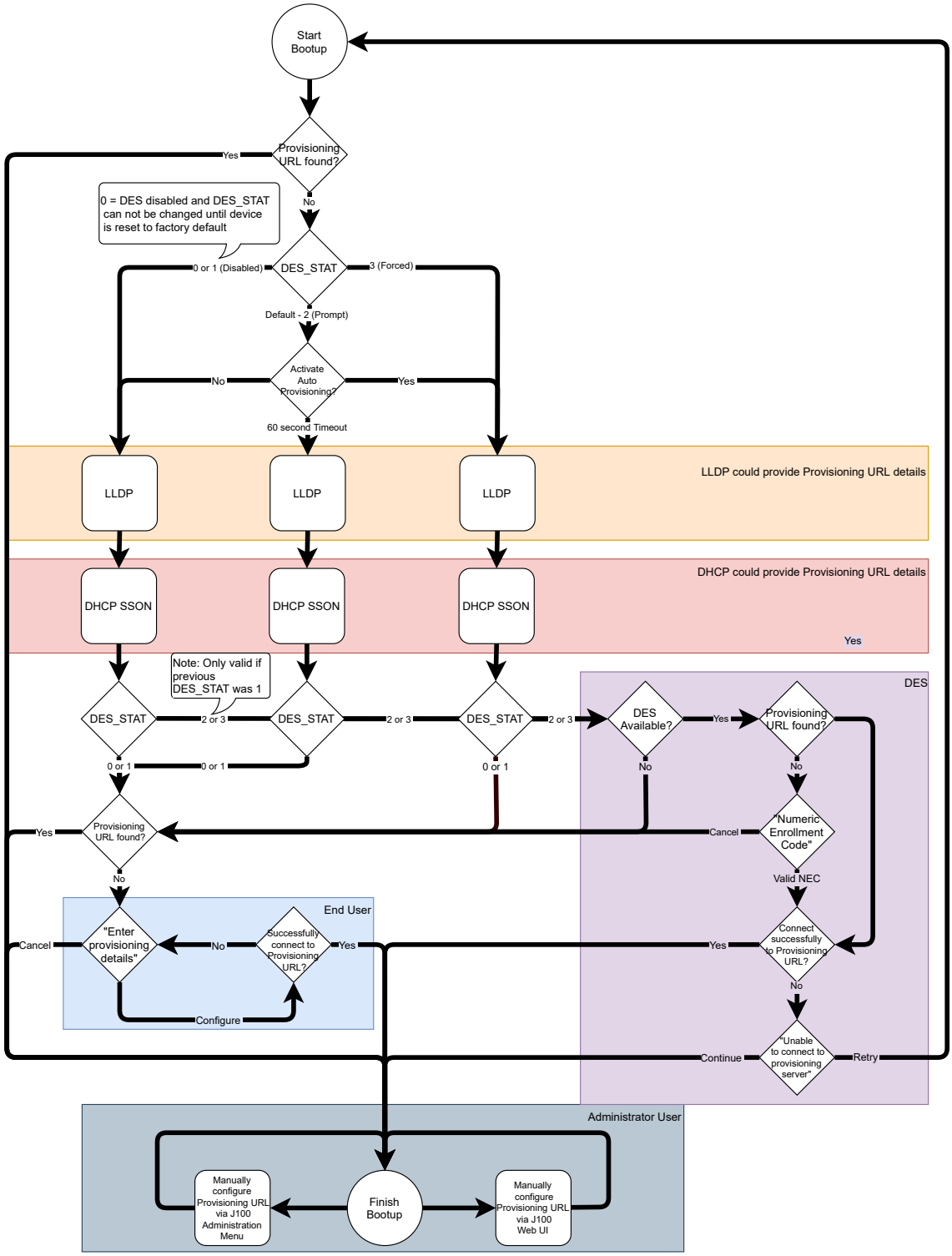
A provisioning server is an HTTP or an HTTPS server that the Avaya J100 Series IP Phones connect to obtain the phone software files and configuration settings files.

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.

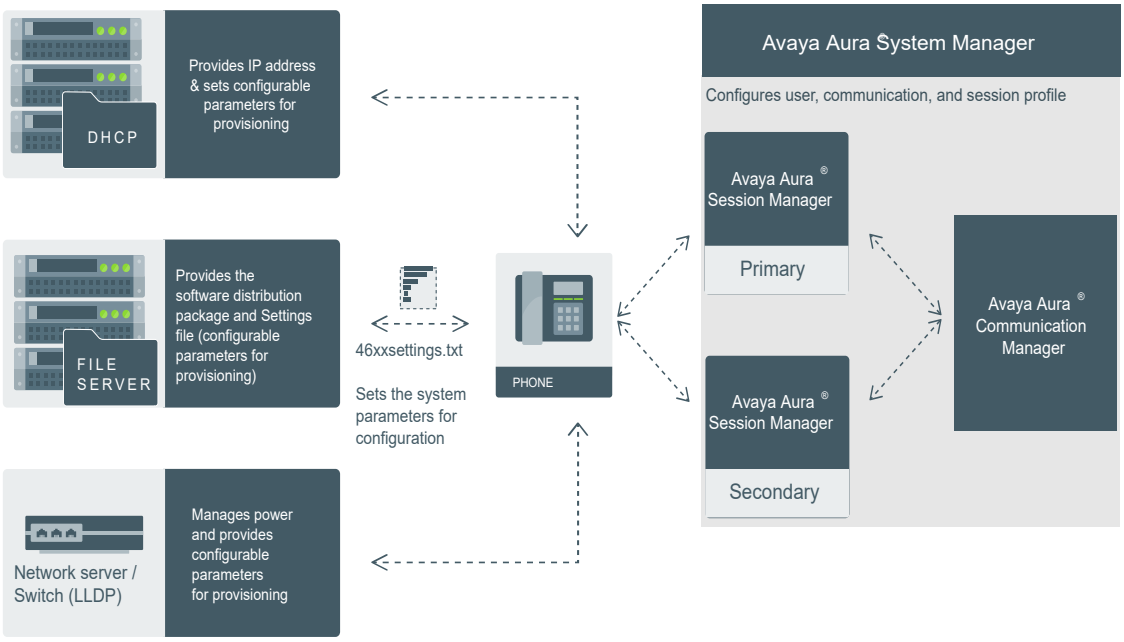
The following methods are available to configure the Avaya J100 Series IP Phones provisioning server address:

- 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:




The following block diagram depicts the provisioning server configuration:




# 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 46

# 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 46

# Configuration through DHCP

The Avaya J100 Series IP Phones obtain network and configuration information using DHCP protocol. You can configure the DHCP server to provide the following information to the device:

- Avaya Aura® Session Manager address.
- IP address
- Subnet mask
- IP address of the router
- IP address of the HTTP or HTTPS file server
- 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.
- Provision device and site-specific configuration parameters through various DHCP options.

## DHCP Site Specific Option

The phones support DHCP configuration option called Site Specific Option(SSON). Using this parameter, custom parameters can be configured on the phone through a DHCP server. In the DHCP DISCOVER, the phone requests for the DHCP Site-specific option (SSON), typically configured in DHCP Option 242. To configure and respond to this request, configure the DHCP server with proper data supplied in the offer for the value of this option. An example of such configuration is as follows:

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

The following parameters can be configured with this feature:

| Parameter | Description |
|---|---|
| ADMIN_PASSWORD | Specifies the security string used to access local procedures.<br>The default is 27238. This is meant to replace PROCPSWD as it provides a more secure password syntax. |
| 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 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 path may contain no more than 127 characters and may contain no spaces. HTTPDIR is the path for all HTTP operations.<br>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 the `SET HTTPDIR=<path>`. |
| HTTPPORT | Sets the TCP port used for HTTP file downloads from non-Avaya servers. The default is 80. |
| HTTPSRVR | IP addresses or DNS names of HTTP file servers used for downloading settings, language, and firmware files during startup.<br>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, that is sends Destination Unreachable messages for closed ports used by traceroute. |
| ICMPRED | Controls whether ICMP Redirect messages are processed. The default is 0, that is, redirect messages are not processed. |
| L2Q | 802.1Q tagging mode. The default is 0 for automatic. |
| L2QVLAN | VLAN ID of the voice VLAN. The default is 0. |
| PHY1STAT | Specifies the speed and duplex settings for the Ethernet line interface. The default value is 1 for auto-negotiate. |
| PHY2STAT | Specifies the speed and duplex settings for the secondary (PC) Ethernet interface. The default value is 1. |
| PROCPSWD | Security string used to access local procedures.<br>The default is 27238. ADMIN_PASSWORD replaces this parameter if ADMIN_PASSWORD is set in the `46xxsettings.txt` file.<br>**Note:**<br>Setting this parameter through PPM is more secure because this file can usually be accessed and read by anyone on the network. |
| REUSETIME | Time in seconds for IP address reuse timeout, in seconds. The default is 60 seconds. |
| SIP_CONTROLLER_LIST | SIP proxy or registrar server IP or DNS addresses that can be 0 to 255 characters, IP address in the dotted decimal name format, separated by commas and without any intervening spaces. The default is null, that is, no controllers. |

*Table continues…*

| Parameter | Description |
|---|---|
| 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 length can be from 0 to 127, without spaces. |
| TLSPORT | Destination TCP port used for requests to https server in the range of 0 to 65535. The default is 443, the standard HTTPS port. |
| TLSSRVR | IP addresses or DNS names of Avaya file servers used to download configuration files. Firmware files can also be downloaded using HTTPS.<br>**Note:**<br>Transport Layer Security is used to authenticate the server. |
| VLANTEST | Number of seconds to wait for a DHCPOFFER on a non-zero VLAN. The default is 60 seconds. |

In an IP Office environment `46xxsettings.txt` and `96x1Supgrade.txt` files are auto generated. There is a provision where you can set up a different file server with your own custom Settings file.

# 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 IP addresses 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 IP addresses with commas with no intervening spaces.<br>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. |

*Table continues…*

| Option | Description |
|---|---|
| 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:<br>`AVohhhhhh`, where:<br>• `AV` stands for Avaya.<br>• `o` is one of the following values based on Object Unique Identifier (OUI) derived from the first three octets of the phone MAC address:<br>- A if OUI is 00-04-0D<br>- B if OUI is 00-1B-4F<br>- E if OUI is 00-09-6E<br>- L if OUI is 00-60-1D<br>- T if the OUI is 00-07-3B<br>- X if the OUI is anything else<br>• `hhhhhh` are the ASCII characters for the hexadecimal representation of the last three octets of the phone MAC address. |
| Option 15 | Specifies the domain name. The domain name is required to resolve DNS names into IP addresses.<br>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.<br>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.<br>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.<br>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). |

*Table continues…*

| Option | Description |
|---|---|
| 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:<br>• 1 for DHCPDISCOVER<br>• 3 for DHCPREQUEST<br>For DHCPREQUEST sent to renew the device IP address lease:<br>• If a DHCPACK is received in response, a log event record is generated with a Log Category of DHCP.<br>• 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. |
| Option 55 | Specifies the parameter request list. Acceptable values are:<br>• 1 for subnet mask<br>• 3 for router IP addresses<br>• 6 for domain name server IP addresses<br>• 7 for log server<br>• 15 for domain name<br>• 42 for NTP servers |
| Option 57 | Specifies the maximum DHCP message size.<br>Set the value to 1500.<br>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 120 | Specifies the IPv4 address. The SIP client uses this address to locate a SIP server. |
| Option 242 | Specifies the site-specific option (SSON). It is optional but cannot be used simultaneously with Option 43.<br>If you do not configure this option, ensure that one of the following parameters is configured appropriately elsewhere:<br>• HTTPSRVR<br>• TLSSRVR |

**Related links**

SNTP server configuration on page 57
Signaling protocol on page 94

## 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 |
| 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.<br>Value operation:<br>• 0: Continue use of the expired DHCP lease if the lease could not be renewed.<br>• 1: Stop using the DHCP lease immediately when it expires, as per the standard.<br>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 |

# 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.<br>Interface number subtype = 3 (system port). Interface number = 1.<br>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. |

*Table continues…*

| Category | TLV Name (Type) | TLV Info String (Value) |
|---|---|---|
| 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. |
| 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. |

*Table continues…*

| System parameter name | TLV name | Impact |
|---|---|---|
| L2QVLAN and L2Q | IEEE 802.1 VLAN Name | The value is changed to the TLV VLAN Identifier. L2Q is set to 1 (ON).<br>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.<br>VLAN Name TLV is ignored if:<br>• The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0.<br>• The current value of L2QVLAN was set by a TIA LLDP MED Network Policy TLV.<br>• 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.<br>L2QVLAN - Set to the VLAN ID in the TLV.<br>L2QAUD - Set to the Layer 2 Priority value in the TLV.<br>DSCPAUD - Set to the DSCP value in the TLV.<br>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.<br>This TLV is ignored if:<br>• The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0.<br>• The Application Type is not 1 (Voice) or 2 (Voice Signaling).<br>• 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.<br>L2QVLAN - Set to the VLAN ID in the TLV.<br>L2QAUD - Set to the Layer 2 Priority value in the TLV.<br>DSCPAUD - Set to the DSCP value in the TLV.<br>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.<br>This TLV is ignored if:<br>• The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0.<br>• The Application Type is not 1 (Voice) or 2 (Voice Signaling).<br>• 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.<br>**Note:**<br>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).<br>If the value of TLV = 2, L2Q is set to 2 (Off).<br>If the value of TLV = 3, L2Q is set to 0 (Auto).<br>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.<br>This TLV is ignored if:<br>• The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0.<br>• The current L2QVLAN value was set by an IEEE 802.1 VLAN name.<br>• The current L2QVLAN value was set by a TIA LLDP MED Network Policy (Voice) TLV. |

# 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 58
DHCP options on page 49
IP configuration field description on page 93
Ethernet settings field descriptions on page 134

# SNTP Parameters

Use the `46xxsettings.txt` 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.<br>Addresses can be in dotted-decimal or DNS name format, separated by commas without any intervening spaces.<br>The list can contain up to 255 characters. |

*Table continues…*

| Parameter name | Default Value | Description |
|---|---|---|
| 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.<br>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.<br>Valid values are 0, 1, or 2. The default value is 1. |
| DSTSTART | 2SunMar2L | Specifies when to apply the offset for daylight savings time.<br>The date and time for applying the offset can be set in the following formats:<br>• `odddmmmht`: for example, `2SunMar2L` which corresponds to the second Sunday in March at 2 AM local time;<br>• `Dmmmht`: for example, `10Mar5L` which corresponds to March 10 at 5 AM local time. |
| DSTSTOP | 1SunNov2L | Specifies when to stop applying the offset for daylight savings time.<br>You can set the date and time when the offset is stopped in the following formats:<br>• `odddmmmht`: for example, `1SunNov2L` which corresponds to the first Sunday in November at 2 AM local time;<br>• `Dmmmht`: for example, `7Nov5L` which corresponds to November 7 at 5 AM local time. |

**Related links**

SNTP server configuration on page 57

# 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, or Administration menu. If the phone fails to discover the configuration server using DHCP SSON, LLDP 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. 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 31

# 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.

**Related links**

VLAN separation on page 61
Configuring an external switch port on page 63
Exceptions to the VLAN forwarding rules on page 64
Special considerations on page 64
VLAN parameters on page 65

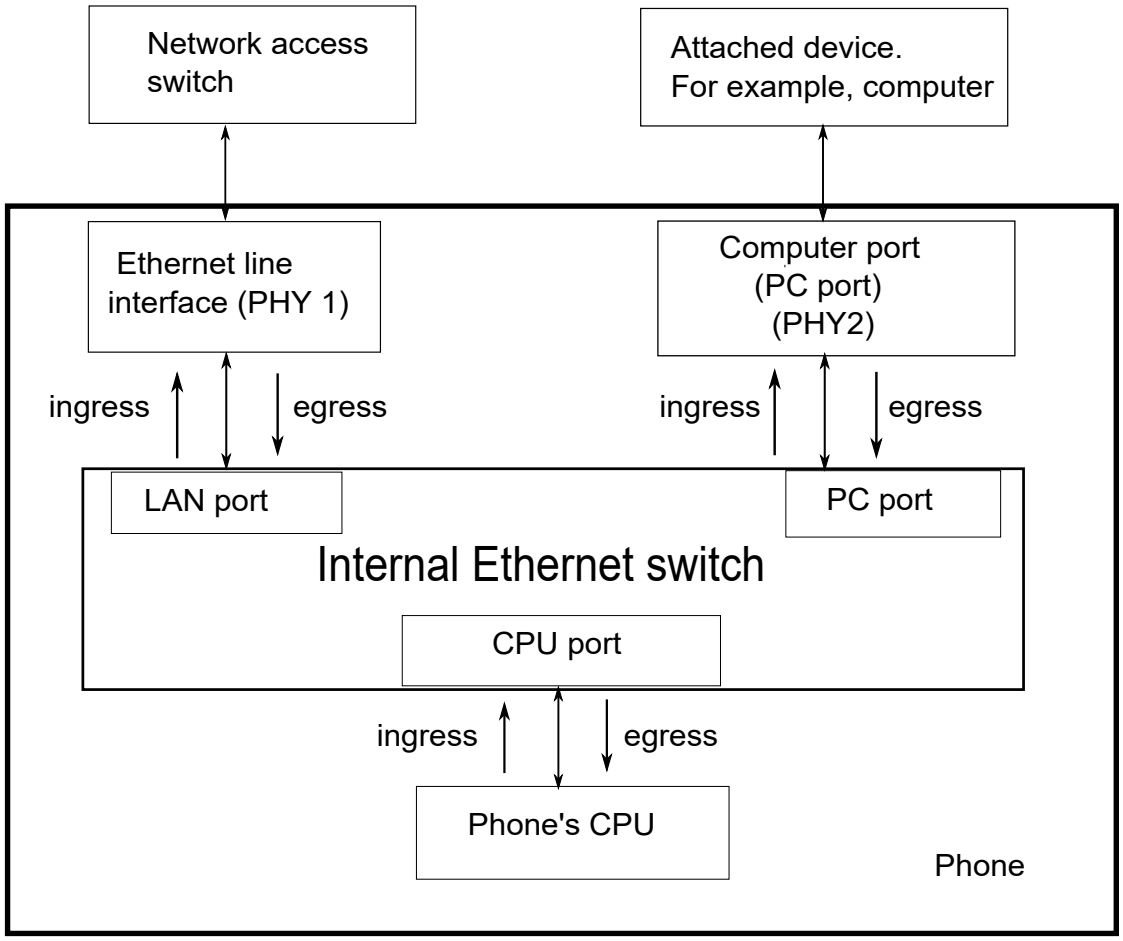
# VLAN separation

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.




**Related links**

[Virtual LAN (VLAN)](#) on page 60
[VLAN separation modes](#) on page 62

## 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.

**Related links**

VLAN separation on page 61

# 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 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 and data VLAN.

**Related links**

Virtual LAN (VLAN) on page 60

# 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

**Related links**

Virtual LAN (VLAN) on page 60

# 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.

**Related links**

Virtual LAN (VLAN) on page 60

# VLAN parameters

The following configuration parameters 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.<br>Value operation:<br>• 0: Auto. VLAN tagging is turned on when the network can support VLAN tagging and L2QVLAN is non zero.<br>• 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.<br>• 2: Off. VLAN functionality is disabled.<br>L2Q is configured through:<br>• Local admin procedure<br>• A name equal to value pair in DHCPACK message<br>• SET command in the `Settings` file<br>• DHCP option 43<br>• 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.<br>Valid values are 0 through 999.<br>Value operation:<br>• 0: The phone continues to attempt a DHCP REQUEST forever.<br>VLANTEST is configured through:<br>• `Settings` file<br>• 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.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled |
| VLANSEPMODE | 1 | Specifies whether the VLAN separation is enabled or disabled.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled<br>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.<br>Value operation:<br>• 0: Strip tags. VLAN tags are stripped from Ethernet frames leaving the computer (PC) port of the phone.<br>• 1: Does not strip tags. VLAN tags are not stripped from Ethernet frames leaving the Computer (PC) port of the phone.<br>PHY2TAGS is configured through the `Settings` file. |
| L2QVLAN | 0 | Specifies the voice VLAN ID to be used by IP phones.<br>Valid values are 0 through 4094.<br>L2QVLAN is configured through:<br>• Local admin procedure<br>• A name equal to value pair in DHCPACK message<br>• SET command in the `Settings` file<br>• DHCP option 43<br>• LLDP |

*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.<br>Valid values are 0 through 4094.<br>PHY2VLAN is configured through:<br>• SET command in a `settings` file<br>• 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.<br>Valid values are 0 through 7.<br>L2QAUD is configured through:<br>• SET command in the `Settings` file<br>• LLDP |
| L2QSIG | 6 | Specifies the layer 2 VLAN priority value for signaling frames generated by the phone.<br>Valid values are 0 through 7.<br>L2QSIG is configured through:<br>• SET command in the `Settings` file<br>• AADS<br>• LLDP<br>Setting this parameter through AADS or LLDP overwrites values in the settings file. |
| PHY2PRIO | 0 | Specifies the layer 2 priority value to be used for frames received on the secondary Ethernet interface when VLAN separation is enabled. The parameter is not supported when VLANSEPMODE is 1.<br>Valid values are 0 through 7.<br>**Note:**<br>J129 does not support this parameter. |

**Related links**

Virtual LAN (VLAN) on page 60

# 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 68

## Received packets (destination = SIP phone)

| Destination port | Source port | Use | Protocol<br>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 TLS/ SSL packets that the HTTP client of the phone sends | Any | TLS/SSL packets that the HTTP client of the phone receives | 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 |

*Table continues…*

| Destination port | Source port | Use | Protocol<br>UDP or TCP |
|---|---|---|---|
| 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 68

# Transmitted packets (source = SIP phone)

| Destination port | Source port | Use | Protocol<br>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 |
| 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 |

*Table continues…*

| Destination port | Source port | Use | Protocol<br>UDP or 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 |

# 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.
- IPv6 only mode.

## IPv6 auto-configuration

The auto-configuration process includes generating a link-local address, global addresses via stateless address auto-configuration (SLAAC), and the Duplicate Address Detection procedure for verifying that the addresses are unique.

On the phone, IPv6 address can be assigned to the interface in the following ways:

- By using DHCPv6
- By using SLAAC
- Manually

For more information, see Configuring IPv6 from the phone menu on page 74.

Both DHCPv6 and stateless address auto-configuration may be used simultaneously.

**Note:**

Do not use DHCPv6 and SLAAC simultaneously for same subnet.

Avaya J100 Series IP Phones can have multiple IPv6 addresses, all of which can be SLAAC.

For more information about configuring parameters for assigning an IPv6 address, see IPv6 configuration on page 72.

# 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)** To exit the menu without saving the changes, press **Cancel**.

# 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 118.
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**.

## 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.<br>Value operation:<br>• 0: DHCPv6 enters proprietary extended rebinding state (continue to use IPv6 address, if DHCPv6 lease expires).<br>• 1: DHCPv6 complies with IETF RFC 8415 standard (immediately release IPv6 address, if DHCPv6 lease expires). |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| DUAL_IPPREF | 4 | DUAL_IPPREF controls the following:<br>• The selection of SSON either from DHCPv4 or DHCPv6 server, when phone is in dual mode, and<br>• Whether an IPv4 or IPv6 addresses returned by DNS would be tried first during dual-mode operation.<br>DHCP clients use DUAL_IPPREF to decide which SSON configuration attributes to apply for DHCPv4/DHCPv6 interworking in dual mode.<br>Value operation:<br>• 4(Default): IPv4 is preferred.<br>• 6: IPv6 is preferred. |
| PRIVACY_SLAAC_MODE | 1 | Specifies the preference for Privacy Extensions.<br>Value operation:<br>• 0: Disable Privacy Extensions.<br>• 1(Default): Enable Privacy Extensions, and prefer public addresses to temporary addresses.<br>• 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.<br>Value operation:<br>• 0: Only IPv4 mode is enabled.<br>• 1(Default): Dual mode is enabled.<br>• 2: Only IPv6 mode is enabled. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| IPV6DADXMITS | 1 | Specifies whether Duplicate Address Detection is performed on tentative addresses, as specified in RFC 4862.<br>Value operation:<br>• 0: DAD is disabled<br>• 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)** To exit the menu without saving the changes, press **Cancel**.

# 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 118.
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**.

# 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 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.

# DNS resolution for SIP controller

With software version R4.0.11 and later, Avaya J100 Series IP Phones support DNS service to lookup a Fully Qualified Domain Name (FQDN) in the host part of the SIP_CONTROLLER_LIST parameter.

To use FQDN format in SIP proxies, configure FQDN in SIP_CONTROLLER_LIST from all or at least one proxy source, such as LLDP, DHCP, and Settings file. Configure DNS server with these FQDN to resolve to the required IPv4 or IPv6 addresses in A/AAAA records.

You cannot configure a combination of FQDN and IP addresses. If you configure at least one FQDN, the phone ignores all the IP addresses configured in SIP_CONTROLLER_LIST from all sources.

The following table shows the example configurations:

| LLDP | DHCP | Settings file | PPM | | | | Aggregate value |
|---|---|---|---|---|---|---|---|
| | | | SM1-FQDN | SM1- IP | SM2-FQDN | SM2- IP | |
| 135.27.151.3x | 135.27.151.2x | svsm03.xyz.com | svsm01.xyz.com | 10.133.67.x | Not configured | 10.133.xx.2 | FQDN<br>svsm01.xyz.com<br>svsm03.xyz.com |
| 135.27.151.3x | 135.27.151.2x | 135.27.151.2xx | svsm01.xyz.com | 10.133.67.x | svsm02.xyz.com | 10.133.xx.2 | IP address<br>10.133.67.x<br>10.133.xx.2<br>135.27.151.2xx<br>135.27.151.2x<br>135.27.151.3x |
| 135.27.151.3x | 135.27.151.2x | 135.27.151.2xx | Not configured | 10.133.67.x | svsm02.xyz.com | 10.133.xx.2 | IP address<br>10.133.67.x<br>10.133.xx.2<br>135.27.151.2xx<br>135.27.151.2x<br>135.27.151.3x |
| 135.27.151.3x | 135.27.151.2x | svsm03.xyz.com | svsm01.xyz.com | 10.133.67.x | svsm02.xyz.com | 10.133.xx.2 | FQDN<br>svsm01.xyz.com<br>svsm02.xyz.com<br>svsm03.xyz.com |

*Table continues…*

| LLDP | DHCP | Settings file | PPM | | | | Aggregate value |
|---|---|---|---|---|---|---|---|
| 135.27.151.3x | 135.27.151.2x | svsm03.xyz.com<br>135.27.151.2xx | svsm01.xyz.com | 10.133.67.x | svsm02.xyz.com | 10.133.xx.2 | FQDN<br>svsm01.xyz.com<br>svsm02.xyz.com<br>svsm03.xyz.com |
| 135.27.151.3x | 135.27.151.2x | svsm03.xyz.com | Not configured | 10.133.67.x | Not configured | 10.133.xx.2 | FQDN<br>svsm03.xyz.com |
| svsm01.xyz.com | 135.27.151.2x | 135.27.151.3x | Not configured | 10.133.67.x | Not configured | 10.133.xx.2 | FQDN<br>svsm01.xyz.com |
| 135.27.151.2x | svsm01.xyz.com | 135.27.151.3x | Not configured | 10.133.67.x | Not configured | 10.133.xx.2 | FQDN<br>svsm01.xyz.com |

**Note:**

If you configure the phone with one or more SIP proxies as FQDN using LLDP, DHCP, or settings file, the phone supports using FQDN from PPM. Otherwise, the phone uses the IP address for SIP proxies from PPM.

### Using the web interface and the phone UI to configure SIP controller

If you configure the value for the SIP controller on both the web interface and the Admin menu of the phone, the phone uses the latest configured value.

If you configure at least one FQDN value, the phone uses it. The following table shows the example configuration:

| Existing effective SIP controller | Configure value from phone UI | Configure value from web interface | New effective SIP controller |
|---|---|---|---|
| No value | 10.133.35.5x | 10.133.35.1xx | 10.133.35.1xx |
| 10.133.35.1xx | 10.133.35.5x | No change | 10.133.35.1xx<br>10.133.35.5x |
| 10.133.35.1xx<br>10.133.35.5x | j100sm1.xyz.com | No change | j100sm1.xyz.com |
| j100sm1.xyz.com | j100sm2.xyz.com | No change | j100sm1.xyz.com<br>j100sm2.xyz.com |

*Table continues…*

| Existing effective SIP controller | Configure value from phone UI | Configure value from web interface | New effective SIP controller |
|---|---|---|---|
| j100sm1.xyz.com<br>j100sm2.xyz.com | No change | 10.133.35.1xx<br>10.133.35.5x | 10.133.35.1xx<br>10.133.35.5x |
| 10.133.35.1xx<br>10.133.35.5x | No change | j100sm1.xyz.com<br>10.133.35.1xx | j100sm1.xyz.com |

To configure FQDN, use parameter SIP_CONTROLLER_LIST in all IP modes- IPv4, IPv6, or Dual stack.

Avaya Aura® environment does not support the DNS query of NAPTR and SRV records.

From the software version 4.0.12 and later, the phone supports SNI when you configure SIP proxy in FQDN format. The phone sends SNI in HTTPS certificate exchange.

The phone ignores the parameter setting FQDN_IP_MAP when you configure SIP proxy as FQDN for SIP TLS connection.

The phone ignores the FQDN SIP proxy configuration when you configure using the parameter SIP_CONTROLLER_LIST_2.

**Warning:**

When you configure SIP proxies using FQDN and deploy a Branch Session Manager(BSM) in the environment, the J100 phones cannot connect to a configured BSM if the phone reboots during a WAN outage and there is no local DNS server to resolve the BSM FQDN.

### Limitation

The phone does not detect the duplicate IP addresses that FQDNs resolve.

For example: If both FQDNs j100sm1.avaya.com and j100sm2.avaya.com resolves into the same IP address 10.133.35.151, the phone does not detect the duplicate IP address, it creates two SIP connections to the same IP address.

# Microsoft® Exchange account integration

You can integrate the Avaya J100 Series IP Phones except for Avaya J129 IP Phone with the Microsoft® Exchange account using the Microsoft® authentication method. After successful authentication, the user Exchange calendar and contacts are integrated with the phone. You can choose to integrate the phone or provide 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 using the Oauth or basic authentication. For basic authentication of the new phone, you have to 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 80

# 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.<br>Addresses can be in dotted-decimal or DNS name format, separated by commas without any intervening spaces.<br>The list can contain up to 255 characters. |
| EXCHANGE_SERVER_SECURE_MODE | 1 | Specifies if HTTPS should be used to contact Exchange servers.<br>Value operation:<br>• 0: Use HTTP<br>• 1: Use HTTPS<br>**Note:**<br>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.<br><br>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.<br><br>When you configure non-forced method, phone user can change the authentication method from the phone user interface and configure the active authentication method.<br><br>Value operation:<br><br>• **0**: Basic authentication (Default)<br>• **1**: OAuth authentication<br>• **2**: Basic authentication- forced<br>• **3**: OAuth authentication- forced<br><br>**Note:**<br><br>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.<br>Value operation:<br>• 0: Office 2003/Office2016 username format. Username=<ExchangeUserDomain\ExchangeUserAccount> or Username=<ExchangeUserAccount> if <ExchangeUserDomain> is empty.<br>• 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.<br>If phone user hasn't configured any user name on the phone user interface then value configured in this parameter would be used.<br>The valid value is a string of up to 255 characters. The default value is empty.<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |
| EXCHANGE_EMAIL_DOMAIN | Null | Specifies the Exchange email domain.<br>The value can contain 0 to 255 characters. |
| EXCHANGE_NOTIFY_SUBSCRIPTION_PERIOD | 180 | Specifies the number of seconds between re-syncs with the Exchange server.<br>Valid values are 0 through 3600. |

*Table continues…*

| Parameter name | Default Value | Description |
|---|---|---|
| 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.<br>The value can contain 0 to 255 characters. |

**Related links**

Microsoft Exchange account integration on page 79

# Chapter 5: Avaya Aura configuration for phones

## SIP phone administration on Communication Manager

The SIP-based calling features in the following table can be invoked directly on Avaya J100 Series IP Phones or using a feature button provisioned using Avaya Aura® Communication Manager. Communication Manager automatically processes other calling features such as call coverage, trunk selection using Automatic Alternate Routing (AAR), or Automatic Route Selection (ARS), Class Of Service/Class Of Restriction (COS/COR), and voice messaging.

**Note:**

- For more information, see *Avaya Aura® Communication Manager Feature Description and Implementation* and other Communication Manager administration documents at the Avaya Support website: http://support.avaya.com/
- For information about IP Office, see IP Office SIP Telephone Installation Notes.

The Avaya SIP solution configures all SIP phones in Communication Manager as off-PBX station (OPS).

| Feature | Survivable operation with third-party proxy | Normal operation with Communication Manager and Session Manager |
|---|---|---|
| 3-Way Conferencing | Yes | No |
| Conference using conference server | — | Yes |
| Automatic Call Back/Cancel | — | Yes |
| Call Forward All Calls – on/off | Yes | Yes |
| Call Hold | Yes | Yes |
| Call Park and Unpark | — | Yes |
| Calling Party Number Block | — | Yes |
| EC500 | — | Yes |
| Malicious Call Trace | — | Yes |

*Table continues…*

| Feature | Survivable operation with third-party proxy | Normal operation with Communication Manager and Session Manager |
|---|---|---|
| Message Waiting Indication | MWI is not available. If the PSTN_VM_NUM parameter is administered, users can gain to the voice mailbox. | Yes |
| Mute alert | Yes | Yes |
| Presence | — | Yes |
| Send All Calls Enable/Disable | — | Yes |
| SSH support | Yes | Yes |
| Third Party Call Forward | — | Yes |
| Third Party Call Forward Busy Don't Answer | — | Yes |
| Attended Transfer | Yes | Yes |
| Transfer upon hang-up | — | Yes |

# SIP phone administration on Session Manager

Avaya J100 Series IP Phones might display a prompt asking for the extension and password during the administration on Avaya Aura® Session Manager. The phones use the extension and password to communicate with Session Manager, which communicates with Avaya Aura® Communication Manager.

For more information, see the following documents at the Avaya Support website: http://support.avaya.com/

- For information about the Communication Manager administration with Session Manager, see the following Session Manager and Avaya Aura® System Manager documents:
  - *Avaya Aura® Session Manager Overview and Specification*
  - *Deploying Avaya Aura® Session Manager*
  - *Upgrading Avaya Aura® Session Manager*
  - *Administering Avaya Aura® Session Manager*
  - *Maintaining Avaya Aura® Session Manager*
  - *Troubleshooting Avaya Aura® Session Manager*
  - *Avaya Aura® Session Manager Case Studies*
  - *Deploying Avaya Aura® System Manager on System Platform*
  - *Deploying Avaya Aura® System Manager*

- *Upgrading Avaya Aura® System Manager on System Platform*
- *Upgrading Avaya Aura® System Manager*
- *Administering Avaya Aura® System Manager*
- *Avaya Aura® System Manager Release Notes*
- Administering Avaya IP Office™ Platform with Manager
- Avaya IP Office™ Platform Solution Description
- Avaya IP Office™ Platform Feature Description

# Personal Profile Manager

Personal Profile Manager (PPM) is a part of the Avaya Aura® Session Manager platform in the Avaya Aura® environment.

It maintains and manages the personal information of the end-user in the session manager. SIP endpoints communicate with PPM to:

- Retrieve configuration information such as dial plans, buttons, and contact lists
- Add or update contacts
- Save device-specific data

To secure the communication between Avaya J100 Series IP Phones and PPM, set the parameter CONFIG_SERVER_SECURE_MODE to 1.

For more information about PPM, see *Avaya Aura® Session Manager Overview and Specification*.

# Avaya Aura® Device Services

Avaya Aura® Device Services acts as a single point of administration for Avaya J100 Series IP Phones. You can use Avaya Aura® Device Services as a file server to host the phone software, certificates, language files, and settings file.

For information about Avaya Aura® Device Services installation and administration, see:

- *Deploying Avaya Aura® Device Services*
- *Deploying Avaya Aura® Device Services*

# Controllers

A controller is a proxy server that routes the calls. A controller, such as Avaya Aura® Session Manager or IP Office, also works as a registrar and an interface between Communication Manager and phones.

# Administering emergency numbers

Set the PHNEMERGNUM configuration parameter in the settings file or in the Session Manager to assign a default emergency number. The phone automatically dials the configured number whenever a user presses the **Emerg** soft key on the Login screen, or the Phone screen, or when the user presses the **Yes** soft key on an Emergency Calling pop-up screen. The phone dials the emergency number even if the phone is locked or the user is not logged in.

In the Avaya Aura® environment, you can configure the parameters in System Manager. You must select the **Allow Unauthenticated Emergency Calls** field in System Manager so that users can dial the emergency number when the phone is not registered. However, when a user logs into an Avaya Aura® environment, only the emergency numbers configured in SMGR will be used by the phone. If the parameters are configured in the `Settings` file, the phone can access the emergency phone numbers when the Aura proxy servers are not available.

The local proxy routes emergency calls from a user at a visited phone so that the local emergency number is called. When PHNEMERGNUM is administered, using the **Emerg** soft key overrides the SPEAKERSTAT parameter setting or a user-selected preferred audio path. This means that even if the Speakerphone is disabled, it becomes the default path when the user presses the **Emerg** soft key.

Avaya J100 Series IP Phones displays an **Emerg** soft key when the phone is not registered or when the phone is locked. When the **Emerg** soft key is pressed, the user can call a primary emergency number. There are three parameters associated with this emergency dialing:

- PHNEMERGNUM: Specifies the primary emergency number that a user calls when the **Emerg** soft key is pressed. Also, by specifying the PHNEMERGNUM parameter a user can dial the emergency number manually.
- ENABLE_SHOW_EMERG_SK: Specifies whether the phone displays **Emerg** soft key when the phone is registered and whether the phone displays a confirmation dialogue box when **Emerg** soft key is pressed.
- ENABLE_SHOW_EMERG_SK_UNREG: Specifies whether the phone displays **Emerg** soft key when the phone is not registered and whether the phone displays a confirmation dialogue box when **Emerg** soft key is pressed.

When the phone is locked or when the user is not logged in, it is possible to configure phones to make emergency calls. Depending upon the configuration parameters and whether the SIP proxy supports emergency dialing, it is possible to enable this functionality in the overall SIP solution.

**Note:**

- When in failover, the Emergency Number must be provisioned on the SIP gateway or the user will not be able to dial it.

- When you toggle between server environments, for example, changing from Avaya Aura® environment to third-party call control, you must reset the phone to the default values.
- In an IP Office environment, the auto-generated `Settings` file does not configure the **Emerg** soft key on the phone. User has to manually dial the emergency number.

# 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 89
Configuring the phone using the web interface on page 115
Configuring the phone using the settings file on page 206
Customization modes on page 210
Pre-configuration of keys on page 212
Soft key configuration on page 217


## 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 logging in on page 92.

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

# Parameters for managing Admin menu

| Parameter name | Default value | Description |
|---|---|---|
| PROCSTAT | 0 | Specifies whether the Admin menu is used for device configuration.<br>Value operation:<br>• 0: Specifies that the phone is administered through the Admin menu.<br>• 1: Specifies that the phone is not administered through the Admin menu. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| PROCPSWD | 27238 | Specifies an authentication code for accessing the Admin menu.<br>Value operation:<br>• 27238: Specifies that the authentication code `27238` is set for accessing the Admin menu.<br>• ASCII numbers between 0–7: Specifies an administrator configured authentication code. You must provide at least four ASCII numbers.<br>• Null: Specifies that no authentication code is required to access the Admin menu. |
| ADMIN_PASSWORD | 27238 | Specifies an authentication code for accessing the Admin menu. If the parameter ADMIN_PASSWORD is set, the parameter PROCPSWD is not used.<br>To provide an authentication code, use any of the following combinations:<br>• Numeric (0–9)<br>• Alphabet in upper-case (A-Z)<br>• Alphabet in lower-case (a-z)<br>• Special characters<br>**Note:**<br>• PROCPSWD supports only numeric values. ADMIN_PASSWORD supports alphanumeric and special characters. Hence, for enhanced security, use ADMIN_PASSWORD instead of PROCPSWD.<br>• You can set the PROCPSWD and the ADMIN_PASSWORD in `46xxsettings.txt` file or Avaya Aura® System Manager. However, ADMIN_PASSWORD is supported on Avaya Aura® System Manager 7.1.0 and later. |
| ADMIN_LOGIN_ATTEMPT_ALLOWED | 10 | Specifies the allowed number of failed attempts for accessing the Admin menu for a duration as specified in the parameter. Valid values are between 1-20. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ADMIN_LOGIN_LOCKED_TIME | 10 minutes | Specifies the duration for lockout when a user reaches the maximum attempts limit for accessing the Admin menu. Valid values are between 5-1440 minutes. |
| WEB_ADMIN_PASSWORD | 27238 | Specifies the password to access the phone through a web browser as an administrator.<br>The value set from the web server interface has a higher priority than the Settings file.<br>If the Web admin password is changed using the web server, then the web admin password set through the settings file is not used until the web admin password is set to default through the phone admin menu or the phone is reset to default.<br>Valid values are from 8-31 alphanumeric characters, including upper, lower, and special characters. |

# Accessing the Admin menu after logging 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 logging in on page 92

## 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.<br>Press the **Toggle** button to select. |
| **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.<br>Press the **Toggle** button to select. |
| **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: | |
| **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 server settings. |
| **STUN Server** | Enter the IP address or fully qualified domain name of the STUN server address. |
| The following parameters are available in the VLAN menu: | |

*Table continues…*

| Configuration Parameter Name | Description |
|---|---|
| **802.1Q** | Choose one of the following options:<br>• **Auto**: Automatic mode.<br>• **On**: Turns on the configuration.<br>• **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 the Auto provisioning menu: | |
| **Service** | Specifies option for auto provisioning. Press **Toggle** to choose the required option:<br>• **Inactive**<br>• **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 57

# 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 49
Updating the signaling protocol on page 95
Parameters for signaling protocol on page 95

## 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 94

## 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.<br>Value operation:<br>• 0: Download the upgrade file for the same signaling protocol that is supported by the current software (default)<br>• 1: Download `96x1Hupgrade.txt` (for H.323 software)<br>• 2: Download `96x1Supgrade.txt` (for 96x1 SIP software) or `J100Supgrade.txt` (for J100 SIP) |

**Related links**

Signaling protocol on page 94

# 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 logging in on page 92

# 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 logging in on page 92

# 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.
- System Manager and Communication Manager through Personal Profile Manager (PPM).

**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 if the LAN Administrator instructs you.

### 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 logging in on page 92

# 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 **Syslog enabled** and press **Toggle** to select.
9. **(Optional)** Scroll to **Syslog server** and enter the IP address or FQDN.
10. **(Optional)** Scroll to **Log server secure** and press **Toggle** to select a secure or non-secure mode to send syslog.
11. Press **Save**.

**Related links**

Accessing the Admin menu after logging in on page 92

# 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|9Z1xxxxxxxxxx|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. |

# Administering enhanced local dialing

Phones automatically prepend a number from the incoming call log or from web pages with a digit to dial an outside number. This feature is called enhanced local dialing (ELD). For example, if you get a call from an international number and want to call back, the phone determines the number to be called and prepends the number to get an outside line. The phone then dials the number.

The following configuration parameters are applicable to this feature:

| Parameter name | Default value | Description |
|---|---|---|
| ELD_SYSNUM | 1 | Specifies whether enhanced local dialing algorithm will be applied for system numbers.<br>Value operation:<br>• 0: Disable enhanced local dialing for system numbers.<br>• 1: Enable enhanced local dialing for system numbers. |
| ENHDIALSTAT | 1 | Specifies if the algorithm defined by the parameter is used during certain dialing behaviors.<br>Value operation:<br>• 0: Disables algorithm.<br>• 1: Enables algorithm, but not for contacts.<br>• 2: Enables algorithm, including contacts. |
| PHNCC | 1 | Specifies the international country code of the Communication Manager call server. For example, 1 for the United States, 44 for the United Kingdom, and so on.<br>Valid values are from 1 to 999. |
| PHNDPLENGTH | 5 | Specifies the internal dial plan number length. For example, if the extension number is 12345, then the dial plan length is 5.<br>This value must match the extension length set on your call server.<br>Valid values are from 3 to 13. |
| PHNIC | 011 | Specifies the international access code.<br>Valid values are from 0 to 4 characters such as numbers 0–9, and special symbols such as star key (*), and pound key (#). |
| PHNLD | 1 | Specifies long distance access code.<br>Valid values are from 0 through 9 and empty string. |
| PHNLDLENGTH | 10 | Specifies the maximum length, in digits, of the national telephone number for the country in which the Communication Manager call server is located.<br>For example, 800-555-1111 has a length of 10.<br>Valid values are from 5 to 15. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| PHNOL | 9 | Specifies the outside line access code.<br>Valid values are from 0 to 2 characters such as numbers 0–9, and special symbols such as star key (*), and pound key (#). |

**Note:**

- The parameter values must be relevant to the location of the Avaya Media Server where the IP phones are registered. For example, if a phone is in Japan and its media server is in the United States, set the PHNCC value to 1 for the United States.
- The digits the phones insert and dial are subject to standard Avaya Media Server features and administration. This includes Class of Service (COS), Class of Restriction (COR), Automatic Route Selection (ARS), and so on.
- Phones will not insert the expected digits when calling back from call history or contacts list if the configured SIP user extension is equal to or longer than the number stored in the call history.
- Phones will not insert the expected digits for contacts that are saved of an inbound call from the call history.

### Enhanced Local Dialing scenarios

The PHNOL parameter is applied without modification in the following scenario:

- ELD is applied to incoming history by setting the ENHDIALSTAT parameter to 1 or 2. A user calls a number from the incoming or missed call history. The number of digits in the number:
  1. Is greater than the national number length (PHNLDLENGTH).
  2. Is greater than the internal number length (PHNDPLENGTH) but lesser than the national number length (PHNLDLENGTH). (PHNDPLENGTH < length of the number < PHNLDLENGTH)

The PHNOL parameter is added to the called number in the following scenario:

- ELD is applied to Contacts by setting the ENHDIALSTAT parameter to 2. A user calls a number from Contacts. The number of digits in the number:
  1. Is greater than the national number length (PHNLDLENGTH), and PHNOL is not equal to the first digit of the number.
  2. Is greater than the internal number length (PHNDPLENGTH), and the length of this number is lesser than the national number length (PHNLDLENGTH). (PHNDPLENGTH < length of the number < PHNLDLENGTH)

PHNOL and PHNLD are applied to the number in the following scenario:

- A user calls a number from the incoming or missed call history (ENHDIALSTAT >= 1) or Contacts (ENHDIALSTAT = 2), and the length of this number is equal to the national number length (PHNLDLENGTH).

  **Note:**

  When the first digit of the called number matches PHNLD, only PHNOL is applied.

# 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 logging in on page 92

# Connecting to a Wi-Fi network

## About this task

Use this procedure to connect the phone to a Wi-Fi network. The phone reboots when you toggle between networks.

## 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. In **Network mode**, use the arrow keys or the **Toggle** soft key to select **Wi-Fi**.
6. Configure the following parameters:
   - **Network config**: Choose **Auto** or **Manual** to connect to a Wi-Fi network automatically or manually.
   - **SSID**: Specifies the network name for the selected Wi-Fi network.
   - **Wi-Fi networks**: Press the **Select** soft key to scan for the available Wi-Fi networks.
7. Use the navigation keys to select a Wi-Fi network and press **Connect**.
8. Press **Save**.

### Related links

Accessing the Admin menu after logging in on page 92

# Configuring SIP settings

## About this task

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

**Note:**

In IP Office the auto generated `J100 settings.txt` includes the settings for the SIP servers and protocols. The settings are based on the SIP values set in the IP Office system configuration.

## 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 to detect the available environment are as follows:

     - **Auto**: Detects the Avaya environment automatically.
     - **Off**: Does not detect the Avaya environment and switches to a non-AST mode.
   - **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.
   - **SIP proxy policy**: Specifies whether the settings of SIP proxy servers are read-only or can be edited by the admin user.

The two modes are as follows:

- **Auto**: The admin user can only view the settings made using Settings file, DHCP, LLDP or PPM.
- **Manual**: The admin user can edit, delete, or create new server properties using Admin menu on the phone or the web interface.

7. Select **SIP proxy policy** to change SIP proxy server 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. Toggle to select the **User ID Field** and press **Save**.
9. Select **SIP proxy list**, shows the IP and FQDN values that are configured using Administration menu or the web interface. The phone highlights the value in use. Use the **Up** and **Down Arrow** keys to view, add, or change the following settings for the value you select.
   - **SIP Proxy**: Specifies the IP address or FQDN for Avaya Aura® Session Manager deployments.
   - **Protocol**: Specifies the type of protocol. The options are TCP, UDP, or TLS.
   - **SIP Port**: Specifies the SIP port. If no value is entered, SIP port uses 5060 as the default port for UDP/TCP or 5061 for TLS.
10. Press **Save**.

**Related links**

Accessing the Admin menu after logging in on page 92

# 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 logging in on page 92

# Using the VIEW administrative option

## About this task

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

## Procedure

1. Press **Main Menu** > **Administration**.
2. In the **Access code** field, enter the admin menu password.
3. Press **Enter**.
4. Select **View**.
5. Press **Back** to return to the main menu.

**Related links**

Accessing the Admin menu after logging in on page 92

# VIEW field description

| Setting | Description | Associated Configuration Parameter |
|---|---|---|
| **Model** | The model of the phone that is set by factory procedures. | MODEL |
| **SW version** | The software version of the phone. | |
| **Backup SW version** | The version of the software backup. | |
| **Button modules** | The connected button module to the phone. Button module is supported only in Avaya J169/ J179 IP Phone and Avaya J189 IP Phone. | |
| **Gateway** | The address of the gateway. | |
| **FIPS** | The FIPS mode is displayed. | FIPS_ENABLED |

*Table continues…*

| Setting | Description | Associated Configuration Parameter |
|---|---|---|
| **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** | The MAC address of the phone. | MACADDR |
| **Wi-Fi MAC** | The MAC address of the WiFi interface of the phone. | |
| **Bluetooth MAC** | The MAC address of the Bluetooth interface 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 |
| **Presence Server**<br>The setting is only available in an Avaya Aura® environment. | The IP address of the presence server. | |
| **Gateway** | The primary gateway out of the list of configured ones. | ROUTER_IN_USE |
| **Gateway(V6)** | The primary gateway is IPv6 out of the list of configured ones. | IPV6STAT |
| **HTTPS Server** | The list of IP or DNS addresses of TLS servers for HTTPS file download, settings file or language files, during start-up procedure. | TLSSRVR |
| **HTTPS Port** | The port number of the HTTPS server. | |
| **HTTPS dir** | The directory of the HTTPS server. | |
| **HTTP Server** | The list of IP or DNS addresses of HTTP servers for HTTP file download, settings file or language files, during startup procedure. | HTTPSRVR |
| **HTTP Port** | The port number of the HTTP server. | |
| **HTTP dir** | The directory of the HTTP server. | |

*Table continues…*

| Setting | Description | Associated Configuration Parameter |
|---|---|---|
| **DNS Server** | The IP address of the DNS server that the phone accessed before successfully. | DNSSRVR_IN_USE |
| **SNTP Server** | The SNTP server that the phone used before to set or update the date and time. | SNTPSRVR_IN_USE |
| **STUN Server** | The STUN server address. | |
| **Product ID** | The device ID of the phone. | |
| **Device type** | The default device type of the phone. | |
| **Server type** | The default server type of the phone. | |

# 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 logging in on page 92

# 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 logging in on page 92

# IEEE 802.1X overview

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

The phone supports the MD5, TLS, and PEAP authentication methods.

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, multicast, and pass-through modes, and proxy logoff for the attached device on the PC port. You can use this procedure to set the operational modes.

### Before you begin

- Make the correct RADIUS server configuration and layer-2 network switch for 802.1x authentication.
- If you require EAP-TLS, pre-install the required identity and trusted certificates on the phone. If you require EAP-PEAP, pre-install the required trusted certificate on the phone. For more information on certificates, see Certificate management.

- You can use the DOT1XSTAT parameter to enable 802.1x on the phone settings file, phone administration menu, or web interface. Ensure 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**
   - **Authentication method**
   - **Username**
   - **Password**
   - **TLS identity**
5. Select the setting that you want to change.
6. Press the **Toggle** soft key or the **Left** and **Right Arrow** keys to cycle through the following settings:
   - For the 802.1x supplicant:
     - **Disabled**
     - **Unicast**
     - **Multicast**
   - For the Pass-thru mode:
     - **Enabled**
     - **Enabled logoff**
     - **Disabled**
   - For the Authentication method:
     - **MD5**
     - **TLS**
     - **PEAP**

When you choose a password-based authentication method, configure the following if required:

- **Username**
- **Password**
- **TLS identity**

7. Press **Save**.

**Related links**

Accessing the Admin menu after logging in on page 92

## 802.1x operational mode settings

| Configuration Parameter Name | Description |
|---|---|
| 802.1x supplicant | |
| **Disabled** | To disable 802.1x supplicant. |
| **Unicast** | To enable 802.1x supplicant in unicast mode. |
| **Multicast** | To enable 802.1x supplicant in multicast mode. |
| Pass-thru mode | |
| **Enabled** | The PC port forwards the 802.1x packets to and from the layer-2 switch connected with the LAN interface of the phone. |
| **Enabled logoff** | The PC port forwards the 802.1x packets to and from the layer-2 switch connected with the LAN interface of the phone.<br>The phone sends an EAP Logoff when the PC is disconnected. |
| **Disabled** | Disables 802.1x forwarding between the PC port and the network switch. Do not select this option if the PC is authenticated over 802.1x. |
| Authentication method | |
| **MD5** | To use the EAP-MD5 authentication method. This is a password-based authentication method. |
| **TLS** | To use the EAP-TLS authentication method.<br>If you use EAP-TLS authentication method, you only need to configure TLS identity later. |
| **PEAP** | To use the EAP-PEAP authentication method. This is a password-based authentication method.<br>When you use the EAP-PEAP authentication, the phone only supports the PEAP Phase 2 authentication method, MSCHAPv2. |
| Password-based authentication method configuration parameters | |

*Table continues…*

| Configuration Parameter Name | Description |
|---|---|
| **Username** | Enter the required username. A valid value is a string with a range of 1-31 characters. As a default Username, the phone displays $MACADDR, which is replaced by its Ethernet MAC address.<br>The supported values include: $MACADDR, $MACADDR_UPPER, $SERIALNO, and $SERIALNO_UPPER. |
| **Password** | Enter the required password. A valid value is a string with a range of 1-31 characters.<br>The supported values include: $MACADDR, $MACADDR_UPPER, $SERIALNO, and $SERIALNO_UPPER. |
| **TLS identity** | Enter the required TLS identity. A valid value is a string with a range of 1-31 characters.<br>The supported values include: $MACADDR, MACADDR_UPPER, $SERIALNO, and $SERIALNO_UPPER. |

# 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 logging in on page 92

# 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. For example: user data stored in PPM or on an external server specified by USER_STORE_URI parameter.

   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 logging in on page 92

# 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
- Web Server
- SIP
- Settings
- Date & Time
- Management
- Password
- Debugging
- Certificates
- Environment Settings
- Background and Screen Saver
- Calendar
- Multicast Paging
- Key Configuration
- Softkey Sets
- 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.

You have to enable access to use 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 **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

## Disabling access to the web interface through the Administration menu of the phone

### About this task

If you are not using the phone web interface, you can disable it.

### 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 **No**.
7. Press one of the following:
   - **Save**
   - **OK**

## 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.<br>The options are:<br>• 0: Disable<br>• 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**

Viewing PHONEKEYLIST parameter details on page 216
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)
   - 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. |

*Table continues…*

| Name | Description |
|---|---|
| **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. |
| **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) | |

*Table continues…*

| Name | Description |
|---|---|
| **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. |
| 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. |
| 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 | |

*Table continues…*

| Name | Description |
|---|---|
| **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. |
| **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<br>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.<br>The operations are:<br>• **Ethernet only**<br>• **Ethernet (preferred, but manual override allowed from Phone UI) (default)**<br>• **Wi-Fi (preferred, but manual override allowed from Phone UI)** |
| 802.1x Authentication | |
| **Supplicant Operating Mode** | Specifies the 802.1x supplicant operating mode.<br>The valid values are:<br>• **Disable(default)**<br>• **Supplicant Enable, responds only to received unicast EAPOL messages.**<br>• **Supplicant Enable, responds to received unicast and multicast EAPOL messages.** |

*Table continues…*

| Name | Description |
|---|---|
| **802.1x Pass-through Operating Mode** | Specifies the 802.1x pass-through operating mode.<br>The valid values are:<br>• **Without proxy logoff (Default)**<br>• **With proxy logoff**<br>• **Disable** |
| **Authentication Method** | Specifies the authentication method used by 802.1x.<br>The valid values are:<br>• **MD5 (Default)**<br>• **TLS**<br>• **PEAP**<br>If you select MD5 or PEAP, configure the Username and Password fields.<br>If you select PEAP, the phone only supports PEAP Phase 2 authentication method MSCHAPv2. |
| **Username** | Specifies the username ID the phone provides to the 802.1x authentication server. The phone uses this value only when the Authentication Method is MD5 or PEAP.<br>The valid value is a string with a range of 1-31 characters. The default value is $MACADDR, the Ethernet MAC address of the phone. |
| **Password** | Specifies the password the phone provides to the 802.1x authentication server. The phone uses this value only when the Authentication Method is MD5 or PEAP.<br>The valid value is a string with a range of 1-31 characters. The default value is NULL. |
| **TLS identity** | Specifies the TLS identity the phone provides to 802.1x authentication server. The phone uses this value only when the Authentication Method is TLS.<br>The valid value is a string with a range of 1-31 characters. The default value is $MACADDR, the Ethernet MAC address of the phone.<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |
| VLAN | |

*Table continues…*

| Name | Description |
|---|---|
| **802.1Q** | Specifies whether layer 2 frames generated by the telephone will have IEEE 802.1Q tags.<br>The valid values are:<br>• Auto (Default): frames will be tagged if the value of L2QVLAN is non-zero<br>• **On: frames will always be tagged.**<br>• **Off: frames will never be tagged.** |
| **VLAN ID** | Specifies the voice VLAN ID to be used by IP telephones.<br>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.<br>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.<br>The valid values are:<br>• **Enable (Default)**<br>• **Disable** |
| **PC Port VLAN ID** | Specifies the VLAN ID to be used by frames forwarded to and from the secondary (PHY2) Ethernet interface.<br>The valid values are 0 through 4094. The default value is 0. |
| **Tags to PC Ethernet Interface** | Specifies whether or not tags will be removed from frames forwarded to the secondary (PC) Ethernet interface.<br>The valid values are:<br>• **Remove (Default)**<br>• **Do not remove** |
| LLDP | |

*Table continues…*

| Name | Description |
|---|---|
| **LLDP** | Specifies whether LLDP is Enable.<br>The valid values are:<br>• **Enable only if LLDP frame is received. (Default)**<br>• **Enable**<br>• **Disable** |
| Ethernet Interface | |
| **Ethernet** | Specifies the speed and duplex settings for the Ethernet line interface.<br>The valid values are:<br>• **Auto-negotiate (Default)**<br>• **10Mbps half-duplex**<br>• **10Mbps full-duplex**<br>• **100Mbps half-duplex**<br>• **100Mbps full-duplex**<br>• **1Gbps full-duplex if supported by hardware** |
| **PC Ethernet** | Specifies the speed and duplex settings for the secondary (PC) Ethernet interface.<br>The valid values are:<br>• **Disabled**<br>• **Auto-negotiate (Default)**<br>• **10Mbps half-duplex**<br>• **10Mbps full-duplex**<br>• **100Mbps half-duplex**<br>• **100Mbps full-duplex**<br>• **1Gbps full-duplex if supported by hardware** |
| **PC Ethernet auto-MDIX** | Specifies whether auto-MDIX is Enable on PHY2.<br>The valid values are:<br>• **Disable**<br>• **Enable (Default)** |
| WiFi Interface | |
| WiFi Control | |

*Table continues…*

| Name | Description |
|---|---|
| **WLAN Network Configuration Mode** | Specifies the Wi-Fi network configuration mode.<br>The options are:<br>• **Automatic (default)**<br>• **Manual** |
| WiFi Setting | |
| **Country** | Specifies the country code to define the Wi-Fi radio parameters permitted by the local regulatory domain.<br>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.<br>The options are:<br>• **Disable (default)**<br>• **Enable** |
| **WLAN Active SSID** | Displays active SSID when Wi-Fi is active. This is an internal parameter.<br>Value format: a sting from 0 to 32 characters. The default value is null. |
| **SSID** | Specifies the SSID string of the Wi-Fi network.<br>Value format: alphanumeric characters and special symbols.<br>**Note:**<br>The space character (ASCII 0x20) is not supported.<br>The default value is null. |
| **Security** | Specifies the WLAN security standard for your Wi-Fi network.<br>The options are:<br>• **None (default)**<br>• **WEP Security**<br>• **WPA/WPA2 security (pre-shared key) security**<br>• **WPA2 Enterprise security (802.1x auth.)** |

*Table continues…*

| Name | Description |
|---|---|
| **WLAN Max Authentication Retires** | Specifies the number of retries that will be attempted to establish a secure connection upon receiving authentication failures.<br>The options are:<br>• **0**<br>• **1**<br>• **2**<br>• **3 (Default)**<br>• **4** |
| WEP | |
| **WEP Key Length** | Specifies the passcode key length for WEP security.<br>The options are:<br>• **64 bit**<br>• **128 bit (default)** |
| **WEP Default Key** | Specifies the default key in your Wi-Fi network.<br>The options are:<br>• **WEP Key 1 (default)**<br>• **WEP Key 2**<br>• **WEP Key 3**<br>• **WEP Key 4** |
| **WEP Key 1** | Specifies the WEP key values in the Wi-Fi network.<br>The valid value is up to 26 alphanumeric characters that can be the following:<br>• **Blank**<br>• **0 – 9**<br>• **A – F**<br>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 |
|---|---|
| **WEP Key 2** | Specifies the WEP key values for the Wi-Fi network.<br>The valid value is up to 26 alphanumeric characters that can be the following:<br>• **Blank**<br>• **0 – 9**<br>• **A – F**<br>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.<br>The valid value is up to 26 alphanumeric characters that can be the following:<br>• **Blank**<br>• **0 – 9**<br>• **A – F**<br>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.<br>The valid value is up to 26 alphanumeric characters that can be the following:<br>• **Blank**<br>• **0 – 9**<br>• **A – F**<br>The value must include 10 hexadecimal digits for 64 bit keys and 26 hexadecimal digits for 128 bit keys. The default value is null. |
| WPA2 Enterprise (802.1x) | |
| **EAP Authentication Method** | Specifies the type of EAP authentication method.<br>The options are:<br>• **PEAP (default)**<br>• **TLS** |

*Table continues…*

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

*Table continues…*

| Name | Description |
|---|---|
| **Destination Unreachable Message Control** | Controls whether ICMP Destination Unreachable messages are generated.<br>The valid values are:<br>• **No**<br>• **Limited Port Unreachable messages (Default)**<br>• **Protocol and Port Unreachable messages** |
| **Redirect Message Control** | Controls whether received ICMP Redirect messages will be processed.<br>The valid values are:<br>• **No(Default)**<br>• **Yes** |
| TCP | |
| **Send TCP Keep Alive Message** | Specifies whether or not the telephone sends TCP keep alive messages.<br>The valid values are:<br>• **Enable (Default)**<br>• **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.<br>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.<br>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.<br>The options are:<br>• **1.0 and 1.2 (default)**<br>• **Only 1.2**<br>• **Only 1.3** |

# 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.<br>The options are:<br>• **IPv4 only**<br>• **Dual mode (Default)**<br>• **IPv6 only** |
| **Dual Mode Operation Preference** | Specifies the preference of the operation mode.<br>The options are:<br>• **IPv4 (Default)**<br>• **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.<br>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.<br>The options are:<br>• **Yes (Default)**: To assign the IPv4 address automatically to your phone.<br>• **No**: To assign the IPv4 address manually to your phone.<br>**Note:**<br>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.<br>The options are:<br>• **Yes (Default)**: To use the assigned IP address after the DHCP lease expires.<br>• **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.<br>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.<br>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.<br>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.<br>The options are:<br>• **DHCPv6 client enabled (Default)**<br>• **DHCPv6 client disabled** |
| **Use DHCPv6** | Specifies whether to use DHCPv6 as a source in IPv6 network.<br>The options are:<br>• **Yes (Default)**: To assign the IPv4 address automatically to your phone.<br>• **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.<br>The options are:<br>• **Yes (Default)**<br>• **No** |
| **IPv6 Address** | Specifies the IPv6 address of the phone.<br>Value format: eight groups of four hexadecimal digits. The default value is null. |
| **IPv6 Link Local Address** | Specifies the link local address.<br>Value format: eight groups of four hexadecimal digits. The default value is null. |
| **IPv6 Gateway** | Specifies the IP address of the gateway.<br>Value format: eight groups of four hexadecimal digits. The default value is null. |
| **Use SLAAC** | Specifies whether to use Stateless Auto-Configuration.<br>The options are:<br>• **Yes (Default)**<br>• **No** |
| **Privacy SLAAC Mode** | Specifies the preference for Privacy Extensions in SLAAC.<br>The options are:<br>• **Disabled, stable address generated from MAC**<br>• **Stable private address (Default)**<br>• **Temporary address** |
| **SLAAC Addresses** | SLAAC (stateless auto configuration) IPv6 addresses.<br>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.<br>The options are:<br>• **Yes (Default)**: To assign the IPv4 address automatically to your phone.<br>• **No**: To assign the IPv4 address manually to your phone.<br>**Note:**<br>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.<br>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.<br>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.<br>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.<br>The valid value is the IP address in the dotted decimal name format, DNS name format or colon-hex.<br>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.<br>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.<br>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.<br>The valid value is the IP address in the dotted decimal name format, DNS name format, or colon-hex.<br>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.<br>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.<br>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.<br>The default value is null. |
| **User Password** | Specifies the password for the HTTP Provisioning Server authentication.<br>The default value is null. |
| DNS | |
| **DNS Server** | Specifies the DNS server address.<br>Valid value is IP addresses in dotted-decimal format, separated by commas without any intervening spaces.<br>The default value is null.<br>You can add up to 16 DNS servers. |
| **DNS Domain** | Specifies the domain name of the DNS server.<br>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.<br>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.<br>The valid value ranges is 60 through 2880 minutes.<br>The default value is 1440 minutes. |
| **GMT Offset** | Specifies the time offset from GMT in hours and minutes.<br>The valid value is a string.<br>The default value is 0:00. |

**Related links**

SNTP server configuration on page 57

# 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.<br>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.<br>The valid value is an integer from 0 to 7. The default value is 6. |
| DiffServe | |

*Table continues…*

| Name | Description |
|---|---|
| **Audio Priority (Layer 3)** | Specifies the layer 3 Differentiated Services (DiffServ) code point for audio frames generated by the phone.<br>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.<br>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.<br>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.<br>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.<br>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.<br>The valid value is an integer from 0 to 63. The default value is 34. |

# 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.<br>The options are:<br>• **No (default)**<br>• **Yes** |
| **HTTP Listen Port** | Specifies the port number of the web server when the web interface is accessed using HTTP.<br>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.<br>The valid value range is from 443 to 65535. The default port number is 443.<br>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.<br>The options are:<br>• **Factory Certificate (default)**<br>• **Custom Certificate** |
| **HSTS** | Specifies whether the phone sends the HTTP Strict Transport Security (HSTS) header in the HTTP response.<br>**Note:**<br>If you enable this value, the phone sends the header only when the web UI is accessed over the HTTPS.<br>The options are:<br>• **Disabled (default)**<br>• **Enabled** |

*Table continues…*

| Name | Description |
|---|---|
| Certificates | |
| **Available Webserver Certificate** | Specifies the trust certificates used as trust points for TLS connections.<br>The valid value must be in `.pem` or `.p12` formats. |
| **Upload Custom Webserver Certificate** | Specifies the custom certificates to be uploaded.<br>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.<br>The valid value is an integer from 0 to 63. The default value is 46.<br>The valid values are:<br>• Enabled (Default)<br>• 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
   - 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.<br>The status can be the following:<br>• Not Configured<br>• Not Registered<br>• Registered |
| **SIP User ID** | Specifies the SIP user ID used to log in to the phone.<br>You can also type the SIP user ID, which is a combination of the following values:<br>• Upper and lower case characters.<br>• Numbers from 0 to 9.<br>• Spaces.<br>• Special characters. The allowed characters are the following: . , : ; “” ‘ / () {} [] ` ~ * _ ! ? + - ^ # = <> \| & $ —<br>The default value is empty. |
| **Authentication User ID** | Specifies the authentication ID.<br>You can also type the authentication user ID in this field if authentication is enabled on the SIP server.<br>The authentication user ID is a combination of the following values:<br>• Upper and lower case characters.<br>• Numbers from 0 to 9.<br>• Spaces.<br>• Special characters. The allowed characters are the following: . , : ; “” ‘ / () {} [] ` ~ * _ ! ? + - ^ # = <> \| & $ — |
| **Authentication Password** | Specifies the authentication password.<br>You can also type the password in this field if authentication is enabled on the SIP server.<br>**Note:**<br>The password can contain maximum 31 ASCII characters. The default value is empty. |

*Table continues…*

| Name | Description |
|---|---|
| SIP Global Settings | |
| **SIP Domain** | Specifies the SIP domain used for SIP registration.<br>The valid value is a string of 0 to 255 ASCII characters. |
| **Enable PPM as source of Proxy Server** | Specifies whether PPM is used as a source of SIP proxy server information.<br>**Note:**<br>This is an Avaya Aura® setting which is ignored in an Open SIP environment.<br>The options are:<br>• **Yes (default)**<br>• **No** |
| **UDP Transport** | Specifies whether UDP transport is allowed.<br>The options are:<br>• **Do Not Allow (default)**<br>• **Allow** |
| **Proxy Policy** | Specifies whether SIP proxy servers are read-only or can be edited.<br>The options are:<br>• **Manual (Use Phone Admin Menu or WEB to configure)**: To configure SIP proxy server manually by using the phone or the web interface.<br>• **Automatic (Can be set from DHCP, LLDP, Settings File, PPM) (default)**: To use the SIP proxy server settings received from the `46xxsettings.txt` file or PPM. |

*Table continues…*

| Name | Description |
|---|---|
| **SIP Proxy Server** | Specifies a list of SIP controller designators.<br>You can set the SIP controllers in FQDNs and IP addresses format. If you set both, FQDNs takes precedence, IP addresses are ignored. When SIP proxy selection policy is Automatic, set the SIP controller in FQDN format in SIP_CONTROLLER_LIST only. If you set the FQDN in the SIP_CONTROLLER_LIST_2, the phone ignores the value.<br>Ensure to set SIP_CONTROLLER_LIST in FQDN format in at least one of the remote sources (LLDP,DHCP,Settings file).<br>If remote sources have any SIP controller in FQDN format, the phone ignores the SIP controllers in IP address format from remote and PPM sources. The help section displays such IP addresses in the precendence table.<br>For any SIP controller FQDN, the phone does not support DNS query of NAPTR and SRV records. The DNS server with the FQDN, resolves to A/AAAA records depending on the IP Mode of the device.<br>In IPv6 deployments if you specify SIP controllers in FQDN format, use SIP_CONTROLLER_LIST and not SIP_CONTROLLER_LIST_2.<br>FQDN_IP_MAP parameter has no effect, if you use SIP controllers in FQDN format. |
| **SIP Proxy Server (Automatic)** | Specifies the SIP proxy server settings as received from the `46xxsettings.txt` file or PPM. |
| **Register to Proxy Server** | Specifies whether the phone registers simultaneously to a proxy server.<br>The options are:<br>• **Simultaneous (default)**<br>• **Alternate** |
| **Number of proxy server to register simultaneously** | Specifies the number of SIP proxy controllers that the phone can register simultaneously.<br>The options are:<br>• **1**<br>• **2**<br>• **3**<br>• **4**<br>• **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.<br>The options range from **1** to **10** line appearances. The default value is **3**. |

*Table continues…*

| Name | Description |
|---|---|
| **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.<br>The options are:<br>• **Enabled**<br>• **Disabled (default)** |
| **Registration Interval** | Specifies the time interval in seconds between two registrations to the SIP proxy.<br>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.<br>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.<br>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.<br>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.<br>The default value is **IPv4**. |
| Codecs and DTMF | |
| **OPUS** | Specifies whether the OPUS codec capability of the phone is enabled or disabled.<br>The options are:<br>• **Disabled**<br>• **Enabled WIDEBAND_20K (default)**<br>• **Enabled NARROWBAND_16K**<br>• **Enabled NARROWBAND_12K** |
| **G.722** | Specifies whether the G.722 codec is enabled.<br>The options are:<br>• **Disable**<br>• **Enable (default)** |

*Table continues…*

| Name | Description |
|---|---|
| **G.726** | Specifies whether the G.726 codec is enabled.<br>The options are:<br>• **Disable**<br>• **Enable (default)** |
| **G.729** | Specifies whether the G.729A codec is enabled.<br>The options are:<br>• **Disable**<br>• **Enable without Annex B support (default)**<br>• **Enable with Annex B support** |
| **G.711u law** | Specifies whether the G.711u law codec is enabled.<br>The options are:<br>• **Disable**<br>• **Enable (default)** |
| **G.711a law** | Specifies whether the G.711a law codec is enabled.<br>The options are:<br>• **Disable**<br>• **Enable (default)** |
| **Send DTMF** | Specifies whether the phone sends DTMF tones in-band as regular audio, or out-of-band using RFC 2833 procedures.<br>The options are:<br>• **In-band**<br>• **Out-of-band (default)** |
| **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.<br>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.<br>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.<br>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<br>Assigning Codec Priority on page 153 |
| RTP | |

*Table continues…*

| Name | Description |
|---|---|
| **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.<br>The options are:<br>• **Yes (default)**<br>• **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.<br>The options are:<br>• **Disable**<br>• **Enable (default)** |
| SRTP | |
| **Media Encryption** | Specifies the crypto suite and session parameters for media encryption.<br>The options are:<br>• **aescm128-hmac80**<br>• **aescm128-hmac32**<br>• **aescm128-hmac80-unauth**<br>• **aescm128-hmac32-unauth**<br>• **aescm128-hmac80-unenc**<br>• **aescm128-hmac32-unenc**<br>• **aescm128-hmac80-unenc-unauth**<br>• **aescm128-hmac32-unenc-unauth**<br>• **none (default)**<br>• **aescm256-hmac80**<br>• **aescm256-hmac32**<br>**Note:**<br>You should not use unauthenticated media encryption (SRTP) options. |
| **Encrypt RTCP** | Specifies whether RTCP packets are encrypted or not.<br>The options are:<br>• **Yes**: SRTCP is enabled.<br>• **No (default)**: SRTCP is disabled. |

*Table continues…*

| Name | Description |
|---|---|
| **Enforce "SIPS" URI for SRTP** | Specifies whether a SIPS URI must be used for SRTP.<br>The options are:<br>• **Yes (default)**: Enforced<br>• **No**: Not enforced. |
| **SDP Negotiation Capability** | Specifies the Session Description Protocol (SDP) negotiation capability.<br>• **Yes (default)**<br>• **No** |
| Voice Quality Monitoring | |
| **RTCP_XR** | Specifies whether and how VoIP Metrics Report Block as defined in RTP Control Protocol Extended Reports (RTCP XR) (RFC 3611) is sent.<br>The options are:<br>• **Disable**: RTCP XR is not sent to remote peers and to any voice monitoring servers.<br>• **Enable for peers and voice monitoring servers**: RTCP XR is sent to remote peers and to any voice monitoring servers<br>• **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.<br>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.<br>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.<br>Valid value is an integer from 5 to 30. The default value is 5 seconds. |
| **RTCP Publish Address** | This parameter is not supported in Avaya Aura®environment. |
| Timers and Count | |
| **SIP Timer T1** | Specifies an estimate in milliseconds for the Round Trip Time (RTT).<br>The valid value is an integer from 500 to 10,000.<br>The default value is 500 milliseconds. |
| **SIP Timer T2** | Specifies the maximum retransmit interval in milliseconds for non-INVITE requests and INVITE responses.<br>The valid value is an integer from 2,000 to 40,000.<br>The default value is 4,000 milliseconds. |

*Table continues…*

| Name | Description |
|---|---|
| **SIP Timer T4** | Specifies the maximum duration in milliseconds for which a message remains in the network.<br>The valid value is an integer from 2,500 to 60,000.<br>The default value is 5,000 milliseconds. |
| **INVITE Response Timeout** | Specifies the maximum number of seconds that the phone waits for another response after receiving a SIP 100 Trying response.<br>The valid value is an integer from 30 to 180.<br>The default value is 60 seconds. |
| **Failed Session Removal Timer** | Specifies the time in seconds to automatically remove a failed call session.<br>The valid value is an integer from 5 to 999.<br>The default value is 30 seconds. |
| **Outbound Subscription Duration Request** | Specifies the outbound subscription request duration in seconds.<br>The valid value is an integer from 60 to 31,536,000.<br>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.<br>The valid value is an integer from 4 to 3,600.<br>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.<br>The valid value is an integer from 16 to 3,600.<br>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.<br>The valid value is an integer from 2 to 3600.<br>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.<br>The valid value is an integer from 2 to 3,600.<br>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.<br>The valid value is an integer from 1 to 30.<br>The default value is 15 attempts. |
| Local Port | |

*Table continues…*

| Name | Description |
|---|---|
| **RTP Port (minimum)** | Specifies the lower limit of a port range.<br>• RTP<br>• RTCP<br>• SRTP<br>• SRTCP<br>The valid value is an integer from 1024 to 65,503.<br>The default value is 2048. |
| **RTP Port (range)** | Specifies the port range to be used by the following connections:<br>• RTP<br>• RTCP<br>• SRTP<br>• SRTCP<br>The valid value is an integer from 32 to 63487.<br>The default value is 40. |
| **SIP Signaling Port (minimum)** | Specifies the lower limit of a port range to be used for SIP signaling.<br>The valid value is an integer from 5062 to 65503.<br>The default value is 1024. |
| **SIP Signaling Port (range)** | Specifies the port range to be used for SIP signaling.<br>The valid value is an integer from 32 to 64511.<br>The default value is 64511. |
| Miscellaneous | |
| **Conference Factory URI** | Specifies the URI for Avaya Aura® Conferencing or network conferencing in Open SIP environments.<br>The valid value is a string of up to 255 ASCII characters. |

*Table continues…*

| Name | Description |
|---|---|
| **Subscribe Event Packages** | Specifies a comma-separated list of event packages to subscribe to after registration.<br>Allowed values are:<br>• `reg`<br>• `dialog`<br>• `mwi`<br>• `ccs`<br>• `message-summary`, which is identical to `mwi`<br>• `avaya-ccs-profile`, which is identical to `ccs`<br>For IP Office, you must use the following:<br>• `reg`<br>• `message-summary`, which is identical to `mwi`<br>• `avaya-ccs-profile`, which is identical to `ccs`<br>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.<br>The options are:<br>• **Disable**: The tag is not included.<br>• **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.<br>The options are:<br>• **Disable (default)**<br>• **Enable** |
| **'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.<br>The options are:<br>• **Display CallerID information (default)**<br>• **Display 'Restricted'** |

*Table continues…*

| Name | Description |
|---|---|
| **Validate host in SIP URI** | Specifies whether to accept SIP URI with unrecognized host part in INVITE message.<br>The valid options are:<br>• **Enable (Default)**: do not accept the SIP URI with unrecognized host.<br>• **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
   - Feature Access Codes (FAC)
   - Phone Menu Options
   - Call Log
   - Contacts
   - LDAP contacts
   - Emergency Call
   - Phone Lock
   - Audio
   - Dialing

- 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
- Presence
- 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**

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.<br>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.<br>Value format: complete language file name from 0 to 32 characters, for example: `Korean.xml`.<br>The default value is empty. |

*Table continues…*

| Name | Description |
|---|---|
| Feature Access | |
| **Call Forward** | Specifies the status of the Call Forwarding feature.<br>The options are:<br>• **Off (default)**<br>• **Unconditional**<br>• **Busy**<br>• **Unconditional and Busy**<br>• **No answer**<br>• **Unconditional and No answer**<br>• **Busy and No answer**<br>• **Unconditional, No answer and Busy** |
| **Number of Ring cycle before Call Forward** | Specifies the number of ring cycles before the call is forwarded.<br>The valid value is an integer from 0 to 20. The default number of ring cycles is 1. |
| **Conference continues on host hangup** | Specifies whether a conference call continues after the host hangs up.<br>The options are:<br>• **Yes**<br>• **No (default)** |
| **Presence** | Specifies the status of the Presence feature.<br>The options are:<br>• **Do Not Allow**<br>• **Allow (default)** |
| **Shortcut action Contact** | Specifies the shortcut action performed by activating the Contact line during an active call.<br>The options are:<br>• **Call to Contact destination (default)**<br>• **Transfer to Contact destination**<br>• **Blind transfer to Contact destination**<br>• **Conference to Contact destination** |

*Table continues…*

| Name | Description |
|---|---|
| **Shortcut action Autodial** | Specifies the shortcut action performed by activating the Autodial line during an active call.<br>Using Autodial line keys as shortcuts is available only in the Avaya Aura® environment.<br>The options are:<br>• **Call to Autodial destination (default)**<br>• **Transfer to Autodial destination**<br>• **Blind transfer to Autodial destination**<br>• **Conference to Autodial destination** |
| **Call Decline policy** | Specifies whether the user can decline the incoming call. You can enable and disable the feature using the following options:<br>The options are:<br>• **Disabled (Default)**<br>• **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.<br>• **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. |
| **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.<br>The options are:<br>• **Disable**: select a higher priority call or reset to select the first line if the phone is idle.<br>• **Enable**: keep the current line selection.<br>The default value is null. |
| **Scrolling mode** | Specifies the scrolling mode on the Phone and Feature screens.<br>The options are:<br>• **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.<br>• **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 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.<br>The options are:<br>• **Yes (Default)**: the softkey1 action is ignored<br>• **No**: the softkey1 action is not ignored.<br>Avaya J129 IP Phone does not support this. |
| **Feature target selection** | Specifies if a user can select a destination number required by a feature using the target options.<br>The options are:<br>• **Disable (Default)**: Disable the feature target selection. You must enter the destination number manually.<br>• **Enable**: Enable the feature target selection. The user can enter the destination number using dial, contacts, recents, and phone button. The user can also use the browser soft key, autodial, busy indicator and team line keys to select the destination number. |
| **SAC ICON** | Use this option to define the icon for SAC feature.<br>The options are:<br>• **DND style (Default)**: Enabling this option allows to use the SAC icon similar to the presence-state DnD icon.<br>• **SAC style**: Enabling this option allows to use an alternate SAC icon. |
| Alerting on calls | |
| Phone Menu Options | |
| **Settings** | Specifies whether the Settings menu is displayed on the phone.<br>The options are:<br>• **Do Not Allow**<br>• **Allow (default)** |
| **Network Info Screen** | Specifies whether the Network Information screen is displayed on the phone.<br>The options are:<br>• **Do Not Allow**<br>• **Allow (default)** |

*Table continues…*

| Name | Description |
|---|---|
| **SIP User Logout** | Specifies whether the Logout feature is provided to the user.<br>The options are:<br>• **Do Not Allow**<br>• **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.<br>The options are:<br>• **Do Not Allow to Modify**<br>• **Allow to Modify (default)** |
| **Restart from Login** | Specifies if the phone displays the Restart soft key from the Login screen. When the user presses the Restart soft key the phone prompts to confirm restart, upon confirmation, the phone restarts.<br>The options are:<br>• **Disable (default)**<br>• **Enable** |
| Call Log | |
| **Call Log** | Specifies whether to enable or disable the Call Log application on the phone.<br>The options are:<br>• **Do Not Allow**<br>• **Allow (default)** |
| **Redial Softkey** | Specifies whether the **Redial** soft key is available.<br>The options are:<br>• **Do Not Allow**<br>• **Allow (default)** |
| **Redial in Phone Menu** | Specifies whether phone redials the last number or displays the list of recently dialed numbers.<br>The options are:<br>• **Do Not Allow (default)**<br>• **Allow** |

*Table continues…*

| Name | Description |
|---|---|
| **Redial Softkey Options** | Specifies whether to show a list or one number on the **Redial** soft key.<br>The options are:<br>• **List (Redial out of list)**<br>• **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.<br>The options are:<br>• **Last number redial (Default)**<br>• **Redial list**<br>• **Last number redialed Forced**<br>• **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.<br>The options are:<br>• **As missed call (Default)**<br>• **As answered call**<br>The default value is as missed call. |
| Contacts | |
| **Local Contacts** | Specifies whether to enable or disable the Contacts application on the phone.<br>The options are:<br>• **Do Not Allow**<br>• **Allow (default)** |
| **Contact Name Format** | Specifies the format of the contact name to be displayed in the Contacts list.<br>The options are:<br>• **'Last Name' 'First Name' (default)**<br>• **'First Name' 'Last Name'** |

*Table continues…*

| Name | Description |
|---|---|
| **Contact Name display logic** | Specifies how to match a dialed string on an incoming call with the users contacts.<br>The options are:<br>• **Match the number completely (default)**<br>• **Match shorter number completely to the rightmost digits of longer number**<br>• **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.<br>The options are:<br>• **Enabled**<br>• **Disable (Default)** |
| **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. |
| **Protocol** | Specifies whether to use TLS or TCP protocol for LDAP.<br>The options are:<br>• **Use LDAP**<br>• **Use LDAP+STARTTLS**<br>• **Use LDAPS (Default)** |
| **Authentication** | Specifies the kind of authentication that is used if the value of the DIRUSERNAME parameter is not null.<br>Value operation:<br>• 0: Simple LDAP authentication.<br>• 1: Simple LDAP Authentication and Security Layer (SASL). |

*Table continues…*

| Name | Description |
|---|---|
| **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.<br>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.<br>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.<br>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.<br>The valid value is a string. Default value is null. |
| 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.<br>The valid value is a string.<br>The default value is fn=firstName,ln=lastName,cn=nickname,telephoneNumber=work |
| Emergency Call | |
| **Emergency Softkey** | Specifies whether the **Emergency** soft key is displayed after the phone is registered.<br>The options are:<br>• **Do Not Display**<br>• **Display without Confirmation**<br>• **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.<br>The valid value is up to 30 dialable characters. The default value is empty.<br>Value format: digits from 0 to 9, *, #. |
| **Emergency Softkey when logged out** | Specifies whether the **Emergency** soft key is displayed when the phone is not registered.<br>The options are:<br>• **Do Not Display**<br>• **Display without Confirmation**<br>• **Display with Confirmation (default)** |
| Phone Lock | |
| **Enable Phone Lock** | Specifies whether the Lock feature is enabled on the phone.<br>The options are:<br>• **Do Not Allow (default)**<br>• **Allow**<br>**Note:**<br>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.<br>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.<br>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.<br>The numeric value ranges between 0–20.<br>If you set the value to 0, the user will not be blocked for the failed attempts to unlock the phone. |

*Table continues…*

| Name | Description |
|---|---|
| **Phone PIN/password lock time** | Specifies the period when the user will be blocked from attempting to unlock the phone.<br>The numeric value ranges between 5–1440 minutes.<br>The default value is 5 minutes. |
| **Phone Lock PIN** | Specifies the PIN that you can set to unlock the phone.<br>The PIN must be only digits with the value ranging from 4–20 characters.<br>The default value is null. |
| Audio | |
| **Call Progress Tone Country** | |
| **AGC Handset** | Specifies the Automatic Gain Control setting for the handset.<br>The options are:<br>• **Disable**<br>• **Enable (default)** |
| **AGC Headset** | Specifies the Automatic Gain Control setting for the headset interface.<br>The options are:<br>• **Disable**<br>• **Enable (default)** |
| **AGC Speaker** | Specifies the Automatic Gain Control setting for the speaker.<br>The options are:<br>• **Disable**<br>• **Enable (default)** |

*Table continues…*

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

*Table continues…*

| Name | Description |
|---|---|
| **Dial Plan** | Specifies the dial plan used in the phone.<br>Value format: a string of 0 to 1023 characters without any intervening spaces.<br>The default value is empty. |
| **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.<br>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`.<br>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.<br>The options are:<br>• **No (default)**<br>• **Yes** |
| **Local Area Code** | Indicates the phone local area code which allows the user to dial local numbers with more flexibility.<br>The valid value is a sting of 5 digits ranged from 0 to 9. The default value is empty. |
| **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.<br>The valid values are:<br>• **Automatic**<br>• **Manual (Default)**<br>• **Automatic Forced**<br>• **Manual Forced** |
| Enhanced Local Dialing Rules | |

*Table continues…*

| Name | Description |
|---|---|
| **Enable Local Dialing Rules** | Specifies whether the algorithm defined by parameters in this section is used during certain dialing procedures.<br>The options are:<br>• **Disable**<br>• **Enable without Contacts (default)**<br>• **Enable with Contacts** |
| **Country Code** | Specifies the country code of the phone.<br>The valid value is an integer from 1 to 999. The default value is 1. |
| **International Access Code** | Specifies the international access code.<br>The valid value is up to 4 dialable characters. The default value is 011.<br>Value format: digits from 0 to 9, *, #. |
| **Long Distance Access Code** | Specifies the long distance access code.<br>The valid value range is a sting of integers from 0 to 9, and empty. The default value is 1. |
| **Internal Extension Number Length** | Specifies the length of an internal extension number.<br>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.<br>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, meaning, a local call in a public network.<br>The valid value is up to 2 dialable characters. The default value is 9.<br>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.<br>The options are:<br>• **No (default)**<br>• **Yes** |
| Admin | |

*Table continues…*

| Name | Description |
|---|---|
| **Admin Access allowed from Phone** | Specifies whether the administrative procedures are used for the phone configuration.<br>The options are:<br>• **Yes (default)**<br>• **No** |
| **Admin Login fail attempt allowed** | Specifies the number of failed attempts to enter the Administration access code before the login is locked.<br>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.<br>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.<br>The options are:<br>• **Disable (default)**<br>• **Enable** |
| **Maximum Precedence Level** | Specifies the maximal allowed precedence level for the user.<br>The options are from 1 to 5. The default value is 1. |
| **MLPP Network Domain** | Specifies the MLPP Network domain.<br>The valid values are: empty, “uc” and “dsn”. The default value is empty. |
| **MLPP Precedence Domain** | Specifies the MLPP Precedence domain.<br>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.<br>The options are:<br>• **Disable**<br>• **Enable (default)** |
| Guest Login | |
| **Guest Login Enable** | Specifies whether the Guest Login feature is available on the phone.<br>The options are:<br>• **Disable (default)**<br>• **Enable** |

*Table continues…*

| Name | Description |
|---|---|
| **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.<br>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.<br>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.<br>The options are:<br>• **Disable (default)**<br>• **Enable** |
| Bluetooth | |
| **Bluetooth Enable** | Specifies whether Bluetooth can be enabled in the phone menu.<br>The options are:<br>• **Disable**<br>• **Enable (default)** |
| CCMS | |
| **Media Preservation** | Specifies whether a call will be preserved when there is no SIP connectivity to IP Office.<br>This setting is applied only in the Avaya Aura® environment.<br>The options are:<br>• **Disable**<br>• **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.<br>This setting is applied only in the Avaya Aura® environment.<br>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.<br>The options are from 1 to 5. The default value is 4. |

*Table continues…*

| Name | Description |
|---|---|
| **Secondary Display Brightness** | Adjusts the brightness of the phone secondary display.<br>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.<br>If no button modules are attached to the phone, this field is disabled.<br>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.<br>If no button modules are attached to the phone, this field is disabled.<br>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.<br>If no button modules are attached to the phone, this field is disabled.<br>The options are from 1 to 5. The default value is 4. |
| **Night Mode Soft key** | Specifies whether the Night mode soft key is available on the phone interface.<br>The options are:<br>• Do Not Allow (Default)<br>• Allow |
| USB<br>This option is available only in Avaya J159 IP Phone and Avaya J189 IP Phone | |
| **USB Power** | Controls USB power when power is provided to the USB interface.<br>The valid values are:<br>• **0-OFF**: turn off USB power.<br>• **1-ON**: turn On USB power only if Aux powered.<br>• **2-ON (Default)**: turn On USB power.<br>• **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.<br>The valid values are:<br>• **Enabled (Default)**<br>• **Disabled** |

*Table continues…*

| Name | Description |
|---|---|
| **USB Keyboard** | Specifies whether to enable or disable USB keyboard. It allows to use the keyboard to enter texts.<br>The valid values are:<br>• **Enabled (Default)**<br>• **Disabled** |
| **USB Stick** | Specifies whether to enable or disable USB stick. It allows to copy phone reports to flash drive.<br>The valid values are:<br>• **Enabled (Default)**<br>• **Disabled** |
| Privacy | |
| **GDPR Mode** | Specifies whether the Secure mode is applied on the phone.<br>The options are:<br>• **Enable (default)**<br>• **Disable** |
| Downloadable Directory | |
| **Downloadable Directory File Name** | Enter the directory file name.<br>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:<br>• Activate the SendAllCall feature when the user enables DoNotDisturb presence.<br>• Activate DoNotDisturb presence when the user enables the SendAllCall feature.<br>• Activate a one-way link between the SendAllCall feature and DoNotDisturb presence.<br>• Disable all links.<br>The options are:<br>• **No link (Do not activate SendAllCall when user enables DoNotDisturb) (Default)**<br>• **One way link (Activate SendAllCall when user enables DoNotDisturb)**<br>• **Two way link (Activate SendAllCall when user enables DoNotDisturb and vice versa)**<br>• **Forced- No link (Do not activate SendAllCall when user enables DoNotDisturb) (Default)**<br>• **Forced- One way link (Activate SendAllCall when user enables DoNotDisturb)**<br>• **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.<br>The options are:<br>• **Disabled**: all Avaya Spaces features through APIs are disabled.<br>• **Guest only (Default)**: Avaya Spaces feature can be accessed by guest/anonymous authentication only.<br>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.<br>The value starts with http:// or https://. The default scheme is https://. The value length is 0- 255 characters without space.<br>The default value is https://spaces.avayacloud.com/<br>**Warning:**<br>Do not change this parameter unless instructed by Avaya Support. |
| **Spaces API URL** | Specifies URL to Avaya Spaces API service.<br>The value starts with http:// or https://. The default scheme is https://. The value length is 0- 255 characters without space.<br>The default value is https://spacesapis.avayacloud.com/api/<br>**Warning:**<br>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.<br>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.<br>The options are:<br>• **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.<br>• **Show (Default)**: user is allowed to select a direct number for a voice call to Avaya Spaces.<br>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.<br>This setting applies only to Avaya J129 IP Phone.<br>The following numbers are assigned to the features:<br>• 0 – Redial<br>• 1 – Contacts<br>• 2 – Emergency<br>• 3 – Recents<br>• 4 – Voicemail<br>Value format: numbers from 0 to 4 and a comma (,).<br>The default value is “0,1,2”. |
| **Branding Volume** | Specifies the volume level at which the Avaya audio brand is played.<br>The options are:<br>• **12db below nominal**<br>• **9db below nominal**<br>• **6db below nominal**<br>• **3db below nominal**<br>• **Nominal (default)**<br>• **3db above nominal**<br>• **6db above nominal**<br>• **9db above nominal** |
| **Phone Mute Alert** | Specifies whether the Mute Alert feature is blocked.<br>The options are:<br>• **Unblocked**<br>• **Blocked (default)** |
| **Extend Ringtone** | Specifies the audio files to customize the ring tone.<br>Value format: the list of file names in `.xml` format separated by commas.<br>The default value is empty. |
| **Group Number** | Specifies group numbers if available.<br>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.<br>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.<br>The options are:<br>• **Do not ignore (Default)**<br>• **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.<br>The options are:<br>• **First Forwarded (Default)**: First user to have forwarded is shown as the Forwarded By User.<br>• **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)<br>The options are:<br>• Minimum value is 0 , the feature is disabled<br>• Maximum value is 30<br>• Default value is 10 minutes |

**Related links**

Active call shortcut keys on page 237

# 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
   - 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 | |
| **DES Discovery** | Specifies the DES Discovery mode.<br>The options are:<br>• **Enable (default)**<br>• **Disable**<br>• **Disable and Restored with Reset to Default**<br>• **Force enable on DES prompt timeout** |

*Table continues…*

| Name | Description |
|---|---|
| **Embedded Public Certificates** | Specifies whether to trust the embedded public certificates.<br>The options are:<br>• **Trusted only if Trustcerts is empty (default)**<br>• **Always Trusted** |
| Configuration | |
| **PPM Server Access Mode** | Specifies the server access mode of the provisioning server.<br>The options are:<br>• **HTTP**<br>• **HTTPS (default)**<br>**Note:**<br>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.<br>The options are:<br>• **Yes**<br>• **No (default)** |
| **Import Settings File** | Enables the user to import the settings file.<br>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**.<br>Restart the phone for new parameters from the settings file to take effect. |
| **Export Settings File** | Enables the user to export a configuration file.<br>To export the configuration file, click **Export**. |
| Firmware | |
| **Software Version** | Displays the version of the SIP software.<br>This field is empty by default. |
| **Backup Software Version** | Displays the backup software version.<br>This field is empty by default. |

*Table continues…*

| Name | Description |
|---|---|
| **Firmware Upgrade** | You can import the firmware upgrade file from a local PC or any PC connected to the network.<br>To upload the firmware upgrade file, click **Browse** to browse your PC, select the file and click **Upgrade**.<br>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.<br>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.<br>The options are:<br>• **Disabled (Default)**<br>• **Daily**<br>• **Weekly**<br>• **Monthly** |
| **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.<br>The options are:<br>• **Don't prompt user (Default)**<br>• **Prompt user if reboot due to new settings or firmware is required** |

*Table continues…*

| Name | Description |
|---|---|
| **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.<br>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.<br>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.<br>Click **Update**, and then click **OK**.<br>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 | |
| **Syslog enabled** | Specifies the enabling or disabling syslog messages.<br>The options are:<br>• **Off (default)**<br>• **On** |

*Table continues…*

| Name | Description |
|---|---|
| **Syslog Server** | Specifies the IP or the DNS address of the Syslog server. For secure syslog mode, you must use an FQDN address.<br>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.<br>The options are:<br>• **Off (default)**<br>• **On** |
| **Log Level** | Specifies the severity level of the syslog messages. Events with the selected severity level and above are logged.<br>The options are:<br>• **Emergencies**<br>• **Alerts**<br>• **Critical**<br>• **Errors (default)**<br>• **Warnings**<br>• **Notices**<br>• **Information**<br>• **Debug** |
| **Log Categories** | Specifies the list of log categories.<br>Select the appropriate log category. For example, select category **Audio** for generating audio logs.<br>The default value is empty. |
| **Enhanced Debugging** | Specifies the status of enhanced debugging.<br>The options are:<br>• **Enable**<br>• **Disable (default)** |
| SNMP | |
| **SNMP String** | Specifies the SNMP community name string.<br>The valid value is a string of up to 32 ASCII alphanumeric characters. The default value is empty. |

*Table continues…*

| Name | Description |
|---|---|
| **SNMP Address** | Specifies the IP addresses for SNMP queries.<br>The valid value is a string of up to 255 ASCII characters without any intervening spaces.<br>The default value is empty. |
| Packet Capture | |
| **Packet Capture** | Captures the phone network traffic.<br>See Capturing the phone network traffic on page 184 |
| Phone Report | |
| **Phone Report Server Address** | Specifies the file server address to send the phone report. Click **Generate Phone Report**.<br>The valid value is a string of up to 255 ASCII characters.<br>**Note:**<br>The phone report also provides details such as product ID, default server type, and Device Enrollment Service (DES) support information. |
| SSH | |
| **SSH Allowed** | Specifies whether Secure Shell (SSH) is supported.<br>The options are:<br>• **Enable**<br>• **Disable (default)**<br>• **Configured using local administrative procedure** |
| **SSH Idle Timeout** | Specifies the time in minutes after which SSH is disabled.<br>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.<br>The valid value is a string of up to 255 ASCII characters. The default value is empty. |
| **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.<br>The valid value is a string of up to 64 ASCII characters. The default value is empty.<br>**Note:**<br>You can add a maximum of four certificates. |

*Table continues…*

| Name | Description |
|---|---|
| **EASG site Authentication Factor code** | Specifies the Site Authentication Factor code associated with the EASG site certificate installed.<br>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 the phone screen displays a warning message for the first.<br>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.<br>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.<br>The options are:<br>• **Disable (default)**<br>• **Enable with payloads removed from RTP packets**<br>• **Enable with payloads included in RTP packets**<br>• **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.<br>The options are:<br>• **Disable (default)**<br>• **Enable**<br>• **Controlled from Admin Menu** |
| **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.<br>The options are:<br>• **Enable**<br>• **Disable (default)** |

*Table continues…*

| Name | Description |
|---|---|
| **UDP Port for discovery and test messages** | Specifies the port used to receive packets from an SLA Monitor server.<br>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.<br>The valid values are:<br>• **Production (Default)**: the dynamic evaluation of the acoustic protection is active.<br>• **Debugging**: the dynamic evaluation of the acoustic protection is inactive. |
| **Acoustic exposure config mode** | Specifies the acoustic exposure dynamic range.<br>The valid values are:<br>• **Acoustic protection off (Default)**<br>• **Acoustic protection On (Default)** |
| **Sliding Window Size** | Specifies the window size for acoustic protection.<br>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.<br>The options are:<br>• **Adjunct**<br>• **Disable**<br>The default value is Adjunct. |

# Capturing the phone network traffic

## About this task

Use the phone network traffic data to debug phone registration and call-related issues. Use the phone web interface to capture the real-time network traffic of the phone. The phone sends the network traffic data to the computer from which 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 network traffic while you run the report.

Use IPv4 network for Avaya J129 IP Phone.

## 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 according to 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.

# Configuring Certificates

### About this task

Use this procedure to configure the required certificates and the related settings. You can also view the list of installed certificates on the phone.

### Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Certificates**.
3. Configure the following areas:

   - Trusted Certificates Configuration
   - Identity Certificates Configuration

   The Certificate field descriptions section provides the details of certificate menus and the option for configuring these areas.
4. Click one of the following:

   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.
5. Select Installed Certificates to view the available certificates on the phone.

## Certificates field descriptions

The following table describes the menu options available on the Certificate tab of the phone web interface:

| Name | Description |
|---|---|
| Installed Certificates | |
| **Installed Trusted Certificate** | Displays all certificates installed through the parameter TRUSTCERTS. |
| **Installed OCSP Trusted Certificates** | Displays all certificates installed through the parameter OCSP_TRUSTCERTS. |
| **Installed Identity Certificates** | Displays all certificates installed through the parameters SCEP, PKCS12URL, and DES. |
| **Installed Custom WebServer Certificate** | Displays custom certificate for WebServer. |
| **Embedded Public Certificates** | Specifies whether the phone is using the embedded public root CA certificates for services other than Device Enrollment Service (DES). |
| Trusted certificates configuration | |
| Certificates | |
| **Upload Trusted Certificate** | Specifies the trusted certificate the phone uses. To browse and upload the certificates from the local PC, click **Import** > **Browse**. |
| **Trusted Certificates file to upload** | Specifies the name of the certificate file to upload on the phone.<br>The valid value is a string up to 255 ASCII characters. File names must be separated by commas without any intervening spaces.<br>The default value is empty. |
| **Match Identity to trust certificate** | Specifies the status of the TLS server identification.<br>The options are:<br>• **Yes (Default)**<br>• **No** |
| **RFC 5922 certificate compliance** | Specifies whether to enable or disable validating the SIP server certificate for RFC 5922 compliance.<br>The options are:<br>• **Enable (Default)**<br>• **Disable** |
| **Require Key Usage certificate extension** | Specifies whether to enable or disable checking for Key Usage extensions.<br>The options are:<br>• **Enable (Default)**<br>• **Disable** |

*Table continues…*

| Name | Description |
|---|---|
| **Server Certificate re-check hours** | Specifies the time interval in hours for rechecking the expiration and revocation status of the certificates that the phone uses to establish any existing TLS connections.<br>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 before which a warning must first appear on the phone screen.<br>The valid value is an integer from 0 to 99. The Default value is 60 days. |
| **FQDN IP Mapping** | Specifies an FQDN available in the certificate when the phone uses an IP address 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.<br>The valid value is a string of up to 255 characters without any intervening spaces. The Default value is empty. |
| Embedded Public Root CA Certificates | |
| Embedded Public Certificates | Specifies whether the phone uses the embedded public root CA certificates for services other than Device Enrollment Service (DES).<br>The options are:<br>• **Not Trusted (Default)**<br>• **Always Trusted** |
| Online Certificate Status Protocol (OCSP) | |
| **Enable OCSP** | Specifies the status of OCSP.<br>The options are:<br>• **Disable (Default)**<br>• **Enable** |
| **Action on Unknown Revocation Status** | Specifies whether a certificate is authenticated when the phone cannot determine the certificate revocation status.<br>The options are:<br>• **Certificate revocation operation will accept certificates (Default)**<br>• **Certificate is considered to be revoked and TLS connection is closed** |

*Table continues…*

| Name | Description |
|---|---|
| **Nonce in OCSP Request** | Specifies whether a nonce is added to OCSP requests and expected in OCSP responses.<br>The options are:<br>• **Do not add**<br>• **Add (Default)** |
| **OCSP Address** | Specifies an URI for an OCSP responder. The URI can be an IP address or a hostname.<br>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.<br>The options are:<br>• **Use OCSP address configured first and then OCSP field of AIA extension of the certificate being checked (Default)**<br>• **Use OCSP field of AIA extension of the certificate being checked first and then OCSP address configured** |
| **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.<br>This value is required if the OCSP responder uses a different CA for the server certificate than the root CA.<br>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.<br>The options are:<br>• **SHA-1 (Default)**<br>• **SHA-256** |
| **Use OCSP Caching** | Specifies whether OCSP caching is in use.<br>The options are:<br>• **Yes (Default)**<br>• **No** |
| **OCSP Cache Expiry** | Specifies the time interval in minutes for the OCSP cache expiry.<br>The valid value is an integer from 60 to 10080. The default value is 2880 minutes. |
| Identity certificates configuration | |
| SCEP Configuration | |

*Table continues…*

| Name | Description |
|---|---|
| **Phone behavior on Pending request** | Specifies the functioning of the device when performing certificate enrollment.<br>The options are:<br>• **Poll SCEP server periodically in background**<br>• **Wait until a certificate is received or rejected (Default)** |
| SCEP #1, SCEP #2, and SCEP #3 (The following fields are common for all three profiles of SCEP certificate) | |
| **SCEP Server** | Specifies the URL address of the SCEP server.<br>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 a SCEP certificate request.<br>The valid value is a string of up to 255 ASCII characters without intervening spaces. The default value is “$SERIALNO”. |
| **Subject** | Specifies the part of SUBJECT in an SCEP certificate request that is common for requests from different devices. For example, Organizational Unit, Organization, Location, State, and Country.<br>The valid value is a string of up to 255 ASCII characters without intervening spaces. The default value is empty. |
| **CA Identifier** | Specifies the Certificate Authority Identifier.<br>Certificate Authority servers might require a specific CA Identifier string to accept GetCA requests. If the phone works with such a Certificate Authority, the CA identifier string can be set through this parameter.<br>The valid value is a string of up to 255 ASCII characters without intervening spaces. The default value is “CAIdentifier”. |
| **Initiate renewal on % of Validity Interval** | Specifies the percentage of the Validity interval of the identity certificate, after which the phone initiates the renewal procedures.<br>If the renewal time interval elapses, the phone starts to contact the SCEP server periodically to renew the certificate.<br>The valid value is an integer from 1 to 90. The default value is 90 percent. |
| **SCEP Password** | Specifies a challenge password to use with SCEP.<br>The valid value is a string of up to 255 ASCII characters without intervening spaces. The default value is “$SERIALNO”. |

*Table continues…*

| Name | Description |
|---|---|
| **SCEP Encryption Algorithm** | Specifies encryption algorithm for SCEP request.<br>The options are:<br>• **DES (Default)**<br>• **AES-256** |
| **SCEP Usage** | Specifies a list of sources for which this certificate should be applied.<br>• **SIP**<br>• **Provisioning**<br>• **802.1x**<br>• **LDAP**<br>• **Ring Central**<br>• **Push**<br>• **PPM**<br>• **XSI**<br>• **Syslog**<br>• **All** |
| PKCS12 #1, PKCS12 #2, and PKCS12 #3 (The following fields are common for all three profiles of PKCS12 certificate) | |
| **PKCS12 Address** | Specifies the IPv4 or IPv6 URL address, or FQDN from where a PKCS#12 file is to be downloaded.<br>The valid value is a string of up to 255 ASCII characters without intervening spaces. The default value is empty. |
| **PKCS12 Password Retry Count** | Specifies the number of attempts for password entry.<br>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.<br>To browse and upload the certificates from the local PC, click **Browse** > **Import**. |

*Table continues…*

| Name | Description |
|---|---|
| **PKCS12 Usage** | Specifies a list of sources for which this certificate should be applied.<br>• **SIP**<br>• **Provisioning**<br>• **802.1x**<br>• **LDAP**<br>• **Ring Central**<br>• **Push**<br>• **PPM**<br>• **XSI**<br>• **Syslog**<br>• **All** |
| DES | |
| **DES Usage** | Specifies a list of sources for which this certificate should be applied.<br>• **Provisioning**<br>• **LDAP**<br>• **Ring Central**<br>• **Push**<br>• **PPM**<br>• **XSI**<br>• **Syslog**<br>• **All** |

# 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 | |
| Primary | |
| **Background Image Selectable by User** | Specifies whether the user can select a primary display background image from phone UI.<br>The options are:<br>• **Enable (default)**<br>• **Disable** |
| **Selected Background Image** | Specifies the file name of the selected primary display background image. The file name must be from the list of background images (see **Background Image List** below).<br>The valid value is a string of up to 255 characters. The default value is empty. |

*Table continues…*

| Name | Description |
|---|---|
| **Background Image List** | Specifies the list of primary display background images.<br>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 display background image from phone UI.<br>The options are:<br>• **Enable (default)**<br>• **Disable** |
| **Selected Background Image** | Specifies the file name of the selected secondary display background image. The file name must be from the list of background images (see **Background Image List** below).<br>The valid value is a string of up to 255 characters. The default value is empty. |
| **Background Image List** | Specifies the list of secondary display background images.<br>The valid value is a string of up to 255 characters separated by commas without any intervening spaces. The default value is empty. |
| Modules | |
| **Background Image Follows Primary Display** | Specifies whether a JEM24 button module must use the same background image as the primary screen.<br>The options are:<br>• **Yes (default)**<br>• **No** |
| **Background Image Selectable by User** | Specifies whether the user can select a JEM24 display background image from phone UI.<br>The options are:<br>• **Enable (default)**<br>• **Disable** |

*Table continues…*

| Name | Description |
|---|---|
| **Selected Background Image** | Specifies the file name of the selected JEM24 display background image. The file name must be from the list of background images (see **Background Image List** below).<br>The valid value is a string of up to 255 characters. The default value is empty. |
| **Background Image List** | Specifies the list of JEM24 display background images.<br>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 display screen saver image from phone UI.<br>The options are:<br>• **Enable (default)**<br>• **Disable** |
| **Selected 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 **Screen Saver Image List** below).<br>The valid value is a string of up to 255 characters. The default value is empty. |
| **Screen Saver Image List** | Specifies the list of primary screen saver images.<br>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 display screen saver image.<br>The options are:<br>• **Enable (default)**<br>• **Disable** |

*Table continues…*

| Name | Description |
|---|---|
| **Selected Screen Saver Image** | Specifies the file name of the selected secondary display screen saver image. The file name must be from the list of screen saver images (see **Secondary Screen Saver Image List** below).<br>The valid value is a string of up to 255 characters. The default value is empty. |
| **Screen Saver Image List** | Specifies the list of secondary display screen saver images.<br>The valid value is a string of up to 255 characters separated by commas without any intervening spaces. The default value is empty. |
| Modules | |
| **Screensaver Image Follows Primary Display** | Specifies whether a JEM24 button module must use the same Screensaver image as the primary screen.<br>The options are:<br>• **Yes (default)**<br>• **No** |
| **Screensaver Image Selectable by User** | Specifies whether the user can select a JEM24 display Screensaver image from phone UI.<br>The options are:<br>• **Enable (default)**<br>• **Disable** |
| **Selected Screensaver Image** | Specifies the file name of the selected JEM24 display Screensaver image. The file name must be from the list of Screensaver images (see **Screensaver Image List** below).<br>The valid value is a string of up to 255 characters. The default value is empty. |
| **Screensaver Image List** | Specifies the list of JEM24 display Screensaver images.<br>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.<br>The options are:<br>• **Enable (Default)**<br>• **Disable** |
| **Admin Configured Authentication Method** | Specifies the Exchange authentication method configured by administrator.<br>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.<br>When you configure non-forced method, phone user can change the authentication method from the phone user interface and configure the active authentication method.<br>The options are:<br>• **Basic (Default)**<br>• **OAuth**<br>**Basic (Forced)**<br>**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.<br>If phone user hasn't configured any user name on the phone user interface then value configured in this parameter would be used.<br>The valid value is a string of up to 255 characters. The default value is empty. |

*Table continues…*

| Name | Description |
|---|---|
| **User Domain (Basic only)** | Specifies the user domain for Microsoft Exchange Server.<br>The valid value is a string of up to 255 characters. The default value is empty. |
| **Email Domain** | Specifies the Exchange email domain for Microsoft Exchange Server.<br>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.<br>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.<br>The default value is empty. |
| **Server Secure Mode** | Specifies the exchange server mode.<br>The options are:<br>• **HTTP**<br>• **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 268
Multicast Paging configuration on page 268

## 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.<br>The options are:<br>• **Enable**<br>• **Disable (default)** |
| **Multicast Paging Codec** | Specifies a codec which will be used in Multicast Paging transmissions.<br>The options are:<br>• **G.729 (default)**<br>• **G.711u**<br>• **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.<br>The configuration fields are equivalent to the MP_GROUPS_TO_LISTEN value:<br>• **IP**: the multicast IP address of the group<br>• **Port**: the IP port of the Multicast Paging group. The valid value is an even integer from 1024 to 65535.<br>• **Priority**: the group priority<br>• **Label**: the group label which the phone displays when the incoming page is played |

*Table continues…*

| Name | Description |
|---|---|
| **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.<br>The configuration fields are equivalent to the MP_GROUPS_TO_SEND value and control the same settings as Multicast Paging Groups To Send fields.<br>• **IP**<br>• **Port**<br>• **Label** |

**Related links**

Multicast Paging configuration on page 268

# 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 this feature using web interface, but it is recommended to use the `46xxsettings.txt` file.

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 or 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 212
Pre-configuration of keys parameter on page 213

## 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:<br>• Keys – 1 to 24 phone keys;<br>• BM 1 (25–48) – 25 to 48 keys of the first attached button module;<br>• BM 2 (49–72) – 49 to 72 keys of the second attached button module;<br>• BM 3 (73–96) – 73 to 96 keys of the third attached button module. |

*Table continues…*

| Name | Description |
|---|---|
| **Type** | Contains the types of key configuration.<br>The values are:<br>• Feature<br>• Application<br>• Line<br>• Autodial<br>• Contact |
| **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. |
| **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. |
| **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. |

*Table continues…*

| Name | Description |
|---|---|
| **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:<br>• Blank<br>• DTMF<br>• Dial<br>• Function<br>• Feature<br>• 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.<br><br>If you try to leave the **Action** field empty for **Dial** or **DTMF**, the phone displays an error message.<br><br>If you have selected **Function** in the **Type** field, you can select between the following functions:<br><br>• Hold<br>• Transfer<br>• End Call<br>• New Call<br>• Conference<br>• Details<br>• Redirect<br>• Emergency<br>• Night<br>• Clear<br>• Dial<br>• Cancel<br>• Complete<br>• Join<br>• Add<br>• Drop<br>• Decline<br>• Ignore<br>• Resume<br>• Barge in<br>• Pick up<br><br>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.<br>• Choose `Replace all softkeys` to display custom softkeys. |

## 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 39.

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 the `J100Supgrade.txt` file then all previously downloaded configuration is cached.
- If the phone is able to download the `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 `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. When parameters of the settings file are removed or are not used, they are reset to the default values.

**Note:**

This procedure does not apply to IP Office environment. In IP Office, the settings file is auto-generated and cannot be modified.

### 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.

**Related links**

List of configuration parameters on page 383

## 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 the `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.

**Note:**

Specifying a language other than English in the configuration file has no impact on Avaya Communication Manager settings, values, or text strings.

# Customization modes

You can configure customization modes to completely or partly block users from customizing phone keys. Available customization modes are the following:

- Blocked: The administrator uses Avaya Aura® System Manager (SMGR) and the PHONEKEY definitions to fully control all phone key customization. The administrator fully controls the phone screen. The phone interprets all values for the PHONEKEY parameter as forced even if you do not configure it.
- Limited: All buttons appear in the same location as you define in SMGR. A user cannot move these buttons but can modify the labels. A user can control Contact and Application favorites.
- Full: Full phone screen customization is available to a user. This is a default mode.

If you select the Limited or Blocked customization mode, you can completely control the system buttons locations on the phone from SMGR without configuring the PHONEKEY parameter. Blocked and Limited modes differ only in the additional user capabilities to control Contact and Application favorites.

In Blocked or Limited mode, you must configure phone keys in Avaya Aura® System Manager (SMGR) and download changes to the phone. The phone forces all the call appearances, bridged appearances, feature buttons, and autodial buttons to appear in the same location. The user cannot delete or move them. For the feature buttons and autodials, only buttons that you mark as favorites are displayed on the main phone screen. You can control where the buttons appear on the phone and prevent users from moving them.

You can configure customization modes in `46xxsettings.txt` or use web UI. The phone applies new settings after log out or reboot.

When you set the Blocked mode, the phone applies the following settings:

- Removes all existing Contact favorites.
- Ignores the PHONEKEY definitions for any SMGR defined buttons.
- Removes all existing Application favorites without PHONEKEY in the settings file.
- Forces SMGR configured buttons to the system-defined locations and removes duplicates.
- Only autodial and feature buttons defined as favorites in SMGR are displayed on the phone.
- To assign a local feature to a line key, you can configure the PHONEKEY parameter in the settings file.

When you set the Limited mode, the phone applies the following settings:

- To assign a local feature to a line key, you can configure the PHONEKEY parameter in the settings file.
- Ignores the PHONEKEY definitions for any SMGR defined buttons.
- Forces all SMGR defined buttons marked as favorites to appear on the line key specified by the SMGR defined location. The phone keeps non-SMGR items if there is no conflict with SMGR settings.

**Related links**

Phone configuration on page 89
Always Favorites on Button Module on page 211
Customization parameters on page 212

# Always Favorites on Button Module

With the Always Favorites on Button Module feature, you can automatically mark all buttons configured in Avaya Aura® System Manager (SMGR) as favorite. A button module displays buttons marked as favorite. When you enable this feature, you cannot remove the favorite flag of a system button that you configured to be on the button module.

When the phone receives a button list from Personal Profile Manager, including at least one configured system button with a button location more than 24, the phone automatically marks the buttons as favorite.

When the button location is more than 24:

- If a Contact or Application occupies the button, the phone removes Contact or Application.
- If another SMGR defined button occupies it, the phone adds the button to the next available empty line key.

You can enable the feature in `46xxsettings.txt` or use web UI. The phone applies new settings after log out or reboot.

**Related links**

Customization modes on page 210
Customization parameters on page 212

## Customization parameters

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

| Parameter name | Default value | Description |
|---|---|---|
| CUSTOMIZATION_MODE | 2 | Specifies the customization mode.<br>Value operation:<br>• 0: Blocked<br>• 1: Limited<br>• 2: Full |
| ALWAYS_FAVORITES_FOR_BUTTON_MODULES | 0 | Specifies whether the Always Favorites on Button Module feature is enabled or not.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled |

**Related links**

Customization modes on page 210
Always Favorites on Button Module on page 211

# 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 for accessing features, applications, or line appearances. You can also set auto-dialing with this feature. You can label configured keys as required.

Pre-configuration of keys is set up for a user or a group of users. The settings apply to all the phones that the user or group use.

In the Avaya Aura® environment, Avaya Aura® System Manager is used to pre-configure automatic dials, call appearances, and features.

You can configure forced or non-forced values for the PHONEKEY parameter. If you select a forced value, the user cannot modify it using the phone interface, and you can modify it only in the `46xxsettings.txt` file. If you do not select the forced value, the user can change key mapping and labels as required, overriding the configuration that the system administrator set.

**Note:**

Using customization modes, you can limit or block the ability of a user to customize their phone screen.

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

- Set the corresponding parameter in the `46xxsettings.txt` file.
- Add the pre-configured keys in the web interface.

It is recommended to configure this feature using the `46xxsettings.txt` file and use Forced parameter values for Avaya Aura®.

**Note:**

The Pre-configuration of keys feature does not support all Avaya Aura® Call Center Elite features.

The IP Office environment does not support the Pre-configuration of keys feature.

**Related links**

Phone configuration on page 89
Phonekey Labels on page 215
Viewing PHONEKEYLIST parameter details on page 216
Keys customization restoration on page 216
Customization modes on page 210
Setting Pre-configuration of keys on page 199
Pre-configuration of keys parameter on page 213

# Pre-configuration of keys parameter

To administer the Pre-configuration of keys feature, you can set the PHONEKEY parameter in the `46xxsettings.txt` file. An administrator can use this parameter to do the following:

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

This parameter is used to map the feature, application, line and auto-dial keys available on the Phone screen. All the PHONEKEY values and keywords are case-insensitive except values set in `Label`.

For the full list of PHONEKEY parameter values and examples of their syntax, refer to their description in Appendix.

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

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

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`.

  **Note:**

  In the Avaya Aura® environment, it is recommended to configure the line keys on Avaya Aura® System Manager.
- `[name]`, depending on the functionality entered in `Type`, it can be either of the following:
  - the feature name that you can access by pressing the customized phone key, e.g., `callfwd` (Call Forward), `team` (Team button), etc.
  - the application name, for example, `lock`, `logout`, `screensaver`, etc.
  - the type of the phone line accessed. The allowed values are: `primary` and`bca` (Bridged Call Appearance).
  - autodialing of a defined phone extension.
- `[label]` is the key label that is displayed on the Phone screen. This setting is optional and case-sensitive.

  You can configure `Label` through the `46xxsettings.txt` file and the Web Interface in the Key Configuration tab.
- `Forced` determines whether the user can move, delete, or relabel a key. This setting is recommended in the Avaya Aura® environment.

  There are several main scenarios for the `Forced` and `Non-forced` settings:
  - 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 and moves it to a different location.
  - 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 closest empty location is selected.
  - If `Forced` is set and you configure **Favorites** using PHONEKEY, and the designated location is occupied by another line key, the new key definition overrides the existing key. The existing key is moved it to a nearest empty location if one is available. If no empty location is available, the new definition overrides the existing key.
  - If `Forced` is not set and you configure **Favorites** using PHONEKEY, and the designated location is occupied by another line key, the new key definition is placed at a nearest

empty location. If no empty location is available, the new definition overrides the existing key.

- If you configure **Favorites** in Forced or Non-forced mode and add a new Favorites entity using PHONEKEY, the existing application or contact which occupies the designated location is replaced only if the new definition is not an application or a contact.
- If `Non-forced` or `Forced` is set and you configure a linekey using the `46xxsettings.txt` file, you cannot delete it using the web interface, but you can move it.

**Related links**

Pre-configuration of keys on page 212
Setting Pre-configuration of keys on page 199
Pre-configuration of keys on page 212
PHONEKEY parameter values on page 510

# Phonekey Labels

In the Avaya Aura® environment, you can configure Label values for the PHONEKEY parameter using the Avaya Aura® System Manager, 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 label 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 212

# 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 212
Viewing IP address of the phone on page 117

# Keys customization restoration

If you set the Full customization mode, the user can restore the customized keys to the administrator settings. When the user selects the restore option, the following happens:

- All buttons that you assign to the phone in SMGR become favorites and are moved to the location defined in SMGR.
- The phone applies PHONEKEYS definitions.
- The phone preserves customized labels except for Applications.
- The phone removes as a favorite any other favorites that are not a SMGR button and are not created from a PHONEKEY definition.

**Related links**

Pre-configuration of keys on page 212
Customization modes on page 210

# 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
- 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

**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.

**Note:**

IP Office in CCMS mode does not support this feature.

**Related links**

Phone configuration on page 89
Configuration of soft key parameter for primary call appearance state on page 218

# 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.<br>For example:<br>`SET SOFTKEY_ACTIVE "type=dtmf;action=##*3;label=Park"`<br>`ADD SOFTKEY_ACTIVE "type=dtmf;action=*34;label=Record"` |

*Table continues…*

| Name | Default | Description |
|---|---|---|
| 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.<br>For example:<br>`SET SOFTKEY_IDLE "type=function;action=newcall;label=call"`<br>`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.<br>For example:<br>`SET SOFTKEY_INCOMING "type=function;action=newcall;label=call"`<br>`ADD SOFTKEY_INCOMING "type=function;action=decline;label=reject"` |
| 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.<br>For example:<br>`SET SOFTKEY_INCOMING_VISUAL "type=function;action=newcall;label=call"`<br>`ADD SOFTKEY_INCOMING_VISUAL "type=function;action=redirect;attr1=65324;label=divert"` |

*Table continues…*

| Name | Default | 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.<br>For example:<br>`SET SOFTKEY_OUTGOING "type=function;action=endcall;label=call"`<br>`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.<br>For example:<br>`SET SOFTKEY_HELD "type=function;action=newcall;label=hold"`<br>`ADD SOFTKEY_HELD "type=function;action=resume;label=drop"` |
| 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.<br>For example:<br>`SET SOFTKEY_DIALING "type=function;action=redial;label=dial"`<br>`ADD SOFTKEY_DIALING "type=function;action=endcall;label=finish"` |

*Table continues…*

| Name | Default | Description |
|---|---|---|
| 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.<br>For example:<br>`SET SOFTKEY_DIALTONE "type=function;action=redial;label=dial"`<br>`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.<br>For example:<br>`SET SOFTKEY_CONFERENCE_DIALING "type=function;action=clear;label=drop"`<br>`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.<br>For example:<br>`SET SOFTKEY_CONFERENCE_OUTGOING "type=function;action=cancel;label=drop"`<br>`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.<br>For example:<br>`SET SOFTKEY_CONFERENCE_CONSULT "type=function;action=cancel;label=drop"`<br>`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.<br>For example:<br>`SET SOFTKEY_CONFERENCE_ACTIVE "type=function;action=cancel;label=drop"`<br>`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.<br>For example:<br>`SET SOFTKEY_TRANSFER_DIALING "type=function;action=clear;label=drop"`<br>`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.<br>For example:<br>`SET SOFTKEY_TRANSFER_OUTGOING "type=function;action=cancel;label=drop"`<br>`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.<br>For example:<br>`SET SOFTKEY_TRANSFER_CONSULT "type=function;action=cancel;label=drop"`<br>`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.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_ACTIVE | 0 | Specifies if the phone shows default softkeys for CA lines in an ACTIVE state.<br>Value operation:<br>• 0: No<br>• 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.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_INCOMING_VISUAL | 0 | Specifies if the phone shows default softkeys for CA lines in an INCOMING_VISUAL state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_OUTGOING | 0 | Specifies if the phone shows default softkeys for CA lines in an OUTGOING state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_HELD | 0 | Specifies if the phone shows default softkeys for CA lines in a HELD state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_DIALING | 0 | Specifies if the phone shows default softkeys for CA lines in a Dialing state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_DIALTONE | 0 | Specifies if the phone shows default softkeys for CA lines in an Dialtone state.<br>Value operation:<br>• 0: No<br>• 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.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_CONFERENCE_OUTGOING | 0 | Specifies if the phone shows default softkeys for CA lines in an Conference Outgoing state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_CONFERENCE_CONSULT | 0 | Specifies if the phone shows default softkeys for CA lines in an Conference Consult state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_CONFERENCE_ACTIVE | 0 | Specifies if the phone shows default softkeys for CA lines in an Conference Active state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_TRANSFER_DIALING | 0 | Specifies if the phone shows default softkeys for CA lines in an Transfer Dialing state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_TRANSFER_OUTGOING | 0 | Specifies if the phone shows default softkeys for CA lines in an Transfer Outgoing state.<br>Value operation:<br>• 0: No<br>• 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.<br>Value operation:<br>• 0: No<br>• 1: Yes |

**Related links**

Soft key configuration on page 217
Soft key parameter values on page 507

# 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 on the phone. 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 230 |
| Contacts | To manage the Contacts list. | Contacts list on page 232 |
| Recents | To manage the call history. | Recents on page 234 |

| 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 call. | Active call shortcut keys on page 237 |
| Automatic Callback | To receive a notification call to connect with the phone extension that was previously unavailable. | Automatic Callback on page 236 |
| Auto Intercom group code | To call a specific intercom group. | Intercom on page 254 |
| Avaya Spaces | To use Avaya Spaces application through the Calendar. | Avaya Spaces Calendar integration on page 238 |
| Busy Indicator | To view the status of the monitored users, make quick calls and transfer to them, and set up conference calls. | Busy Indicator on page 240 |
| Call Decline Policy | To decline an incoming call. | Call decline policy on page 240 |

*Table continues…*

| Feature name | Description | Reference |
|---|---|---|
| Call Forward | To divert incoming calls to another phone extension. | Call Forward on page 241 |
| Calling Party Number Unblocking | To display the user's phone extension during calls. | Calling party number unblocking on page 243 |
| Calling Party Number Blocking | To prevent the phone extension from displaying to other users during calls. | Calling party number blocking on page 243 |
| Call Park | To put an active call on hold and to retrieve this call from another phone. | Call Park on page 242 |
| Call Pickup | To answer an incoming call on behalf of another call pickup group member. | Call Pickup on page 242 |
| Call Recording | To record the call. | Call recording on page 243 |
| Digit mapping | To configure dial plan and dialing rules. | Digit mapping on page 244 |
| Exclusion | To prevent other users from bridging in to the same extension for an existing call. | Exclusion on page 250 |
| Extension to Cellular | To move an incoming call from your deskphone to your personal phone. | Extension to Cellular on page 249 |
| Guest Login | To allow a guest user to log in to another user's primary phone. | Guest login on page 253 |
| Hunt Group Busy | To opt-in and opt-out of the calls specific to the hunt group. | Hunt Group Busy Position on page 254 |
| LDAP Directory | To search global contacts through an LDAP server. | LDAP Directory on page 256 |
| Limit Number of Concurrent Calls | To control the number of concurrent incoming calls. | Limit Number of Concurrent Calls on page 255 |
| Long-term acoustic protection | To protect the headset user's hearing. | Long-term acoustic protection on page 255 |
| Malicious Call Trace | To track a malicious or threatening call. | Malicious call tracing on page 270 |
| MLPP | To override other calls with a priority call. | Multiple Level Precedence and Preemption on page 266 |
| Multiple Device Access | To simultaneously register up to 10 SIP devices for one user. | Multiple Device Access on page 263 |
| Multicast Paging | To send a multicast page to a group of phones. | Multicast Paging on page 268 |

*Table continues…*

| Feature name | Description | Reference |
|---|---|---|
| No Hold Conference | To set up a conference call without putting the existing call on hold. | No Hold Conference on page 271 |
| Pre-configuration of keys | To configure a set of phone keys for accessing features, applications or line appearances. | Pre-configuration of keys on page 212 |
| Presence | To view the status of contacts. | Presence on page 273 |
| Priority Call | To place an important outgoing call with a distinctive ring. | Priority Calling on page 276 |
| Prioritization of codecs | To set priority of use for all codecs. | Prioritization of codecs on page 276 |
| Push | To allow trusted applications to send their content to the phone. | Push on page 277 |
| Send All Calls | To redirect incoming calls to a pre-configured extension. | Send All Calls on page 283 |
| Server-initiated update | To update the phone firmware with new settings. | Server-initiated update on page 284 |
| Team Button | To monitor the status of other team members, answer incoming calls or speed-dial a call to the monitored station. | Team Button on page 286 |
| Voicemail | To listen to your voice mail messages. | Voicemail on page 291 |
| Whisper Page | To make an announcement to a person on a call with the other users having the same extension. | Whisper Page on page 295 |
| WML browser | To view pre-configured WML pages from the phone menu. | WML browser on page 292 |

# 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 exchange reminders are displayed.<br>Value operation:<br>• 0: Not displayed<br>• 1: Displayed<br>**Note:**<br>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.<br>Valid values are 0 through 60.<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |
| EXCHANGE_AUTH_USERNAME_FORMAT | 0 | Specifies the necessary format of the username for http authentication.<br>Value operation:<br>• 0: Office 2003/Office2016 username format. Username= <ExchangeUserDomain\ExchangeUserAccount> or Username= <ExchangeUserAccount> if <ExchangeUserDomain> is empty.<br>• 1: Office 365 format. Username= <ExchangeUserAccount@ExchangeUserDomain> 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.<br>Valid values are 0 through 60. |

*Table continues…*

| Parameter name | Default Value | Description |
|---|---|---|
| EXCHANGE_REMINDER_TONE | 1 | Specifies whether a tone is generated the first time an Exchange reminder is displayed.<br>Value operation:<br>• 0: Tone not generated<br>• 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.<br>The value can contain 0 to 255 characters. |
| PROVIDE_EXCHANGE_CALENDAR | 1 | Specifies if menu items are displayed for exchange calendar.<br>Value operation:<br>• 0: Not displayed<br>• 1: Displayed (default) |
| PROVIDE_EXCHANGE_CONTACTS | 1 | Specifies if menu items are displayed for exchange contacts.<br>Value operation:<br>• 0: Not displayed<br>• 1: Displayed (default) |
| USE_EXCHANGE_CALENDAR | 0 | Specifies whether the calendar synchronizes with Microsoft Exchange.<br>Value operation:<br>• 0: To disable synchronization<br>• 1: To enable synchronization |

**Related links**

Microsoft Exchange account integration on page 79
Microsoft Exchange account integration configuration parameters on page 80

# 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.

## 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.

## 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.<br>Value Operation:<br>• 0: No. The phone disables the **Contacts** option on the interface<br>• 1: Yes<br>**Note:**<br>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. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ENABLE_MODIFY_CONTACTS | | Specifies if the list of contacts and the function of the contacts application can be modified on the phone.<br>Value Operation:<br>• 0: No<br>• 1: Yes |
| USER_STORE_URI | | Specifies the URI path of HTTP/HTTPS server for storing user data. |

# 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. To retain the call log details, enable the offline call log feature in System Manager before downgrading the software.

## 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.<br>The options are:<br>• 0 = Redial<br>• 1 = Contacts<br>• 2 = Emergency<br>• 3 = Recents<br>• 4 = Voicemail<br>**Note:**<br>Open SIP environment does not support emergency calls. |
| ENABLE_CALL_LOG | 1 | Determines whether call logging and associated menus are available on the phone.<br>**Note:**<br>Set this parameter to 0 to keep the user's data private before the user can access the phone. |

# Agent Greeting

With the Agent Greeting feature, call center agents can record customized messages and manually or automatically play them back to callers. Users can configure up to six greeting messages, each message up to 10 seconds long, and save them on the phone.

As an administrator, you can configure whether the phone deletes or keeps the messages when the agent logs out. You can also configure a backup location for the recorded messages using the following configuration parameter:

```
SET BRURI <server URL>
```

Agents can access and automatically download their messages when they log on to another phone.

Agent greeting is available on Avaya J169/J179 IP Phones and Avaya J189 IP Phones.

## Agent Greeting parameters

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

| Parameter name | Default Value | Description |
|---|---|---|
| AGTGREETINGSTAT | 0 | Enables or disables the Agent Greeting feature.<br>Values:<br>• 0: Disabled<br>• 1: Enabled |
| AGTGREETLOGOUTDEL | 5 | Specifies whether the phone deletes agent greeting messages when the agent logs out.<br>• 0: The phone deletes agent greeting messages.<br>• 1: The phone stores agent greeting messages. |
| AGENTGREETINGSDELAY | 0 | Specifies the delay time between call pick up and agent greeting playback.<br>Valid values are 0-3000 milliseconds |

# Feature configuration

## Automatic Callback

The Automatic Callback feature is used to receive a notification call to connect with the available extension number that was previously busy, unanswered, on another call, or out of coverage.

**Note:**

The Automatic Callback feature can be used only when the receiver leaves the call unattended.

This feature must be activated on the Avaya Aura® Communication Manager.

### Automatic Callback configuration

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

| Parameter name | Default value | Description |
|---|---|---|
| CLDELCALLBK | 1 | Specifies whether a call log entry is deleted when a user presses the **Call** softkey from the Details screen to initiate a call back. |

# Active call shortcut keys

With the Active call shortcut keys feature, the users can use Autodial and Contacts keys as shortcuts to perform a specific action during an active call.

Using Autodial keys as shortcuts is available only in the Avaya Aura® 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 (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.

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 154

## 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_CONTACT | 0 | Specify the action performed if the user presses an Autodial key or selects a contact on the Phone screen during an active call.<br>Valid values:<br>• 0: the active call is put on hold, and the destination extension number is dialed.<br>• 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).<br>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.<br>• 2: the active call is immediately transferred to the destination. If this value is used, it overrides |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| SHORTCUT_ACTION_AUTODIAL | | the ENABLE_BLIND_TRANSFER parameter value.<br>• 3: the active call is put on hold, and the call is established with the destination to set up a conference. |

# 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.

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.<br>The options are:<br>• 0: Disabled, all Avaya Spaces features via APIs are disabled.<br>• 1: Guest only, Avaya Spaces feature can be accessed by guest/anonymous authentication only.<br>Connections to Avaya Spaces uses the embedded public certificates and any certificates defined in the TRUSTCERTS. It ignores ENABLE_PUBLIC_CA_CERTS. |

*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, this defined direct number is used.<br><br>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 (+). |
| SPACES_DIRECT_NUMBER_PROVIDE | 1 | Specifies if the end-user can select a direct number for a voice call to Avaya Spaces.<br><br>The options are:<br><br>• 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.<br><br>• 1: Show, the user can select a direct number for a voice call to Avaya Spaces.<br><br>**Note:**<br><br>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 154

# Busy Indicator

With the Busy Indicator feature, the user can view idle or busy status of other users, and make quick calls to them. The icon next to the Busy Indicator line key reflects the current state of the monitored user.

In addition to icons, the indication of LEDs integrated into the Busy Indicator line keys shows the monitored user status. No LED indication corresponds to the idle state of the user. If the monitored user is busy, the right LED integrated into the line key lights green.

The user can also transfer calls to the monitored line, and make conference calls with the monitored user. The Busy Indicator key labels can be customized as required using the Phone keys customization menu.

Busy Indicator is configured on the Avaya Aura® System Manager. However, Busy Indicator line keys can be relabelled and set to a specific location using the Pre-configuration of keys feature.

**Note:**

This feature is available only in the Avaya Aura® environment.

### Busy Indicator limitations

The following are the limitations for the Busy Indicator feature:

- Do not add more than 48 Busy Indicator lines per phone due to possible low performance.
- On the Avaya Aura® 7.1.3.3 – 8.1.1, use 96x1 template in the Communication Profile of a monitoring user. In this case, however, the label customization on the phone might not be synchronized with the labels set on the Avaya Aura® System Manager.

**Related links**

PHONEKEY parameter values on page 510

# 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
- Shared call appearance
- BroadWorks Anywhere
- BroadWorks Mobility

Avaya J129 IP Phone does not support this feature.

## Call decline parameters

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

| 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:<br>The options are:<br>• **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.<br>• **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.<br>• **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

With the Call Forward feature, users can divert incoming calls to another number. You must enable and configure the options for the user to use the Call Forward feature.

The phone supports the following call forwarding options:

- Call Forward: Forwards all incoming calls to another number.
- Call Forward Busy: Forwards incoming calls to another number if the phone line is busy.
- Call Forward No Answer: Forwards incoming calls that are unanswered within a stipulated time to another number.

Enable and configure the Call Forward feature on Avaya Aura® Communication Manager. Depending on the user requirements, you can configure the call forwarding options. A user cannot have the Call Forwarding All Calls capability and the Call Forward Busy and No Answer capability active simultaneously.

### Enhanced Call Forward

With the Enhanced Call Forward feature, the user can divert incoming calls to different numbers depending on the source. When you enable the feature, users can set the rules as per their requirements to forward the internal and external incoming calls. Or, you can configure internal and external phone numbers to the corresponding call forward types.

Enable and configure the Enhanced Call Forward feature on Avaya Aura® Communication Manager.

## 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 **Call Forward**, click one of the following:
   - **Allow**: To enable call forwarding.
   - **Do not allow**: To disable call forwarding.

# Call Pickup

With the Call pickup feature, users can answer an incoming call on behalf of another call pickup group member. You must add members to a call pickup group so that any member of the group can receive a call.

You can add a user to a call pickup group extension, so that the user can redirect an incoming call of a group member to their own phone. If the call pickup feature is active, the call appearance displays an incoming call of the group member on the users phone.

You must activate the call pickup feature on Avaya Aura® Communication Manager.

The Call pickup feature offers the following enhancements:

- Call pickup extended: A member of a pick-up group can also answer a call of a separate pickup group by dialing their group extension number.
- Call pickup directed: A user can receive an incoming call of a specific member of a separate pickup group by dialing in the extension number of the ringing phone.

# 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.

You can activate this feature on Avaya Aura® Communication Manager.

# Calling party number blocking

With the Calling Party Number (CPN) Block feature, users can prevent their number from displaying on the dialed phones. This feature overrides the default system settings to display the extension on outgoing calls.

You must activate this feature on Avaya Aura® Communication Manager.

# Calling party number unblocking

With the Calling Party Number (CPN) Unblock feature, the phone or extension number of the users can be display again on the dialed phones. If you have activated the Calling Party Number Block feature, you can change the settings back to enable displaying the extension.

You must activate CPN Unblock on Avaya Aura® Communication Manager.

# Call recording

With the Audix One-Step Recording feature, the user can record a current call. The AUDIX One-Step Recording feature uses Communication Manager Messaging to record a telephone conversation. A user needs to press a feature button on the phone to activate this feature.

For more information, see Avaya Aura® Communication Manager documentation at https://support.avaya.com/.

## Call recording parameters

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

| Parameter name | Default Value | Description |
|---|---|---|
| RECORDINGTONE_INTERVAL | 15 | Specifies the number of seconds between call recording tones.<br>Valid values are 1 through 60. |

*Table continues…*

| Parameter name | Default Value | Description |
|---|---|---|
| RECORDINGTONE_VOLUME | 0 | Specifies the volume of the call recording tone in 5dB steps.<br>Value operation:<br>• 0: The tone volume is equal to the transmit audio level (default).<br>• 1: The tone volume is 45dB below the transmit audio level.<br>• 2: The tone volume is 40dB below the transmit audio level.<br>• 3: The tone volume is 35dB below the transmit audio level.<br>• 4: The tone volume is 30dB below the transmit audio level.<br>• 5: The tone volume is 25dB below the transmit audio level.<br>• 6: The tone volume is 20dB below the transmit audio level.<br>• 7: The tone volume is 15dB below the transmit audio level.<br>• 8: The tone volume is 10dB below the transmit audio level.<br>• 9: The tone volume is 5dB below the transmit audio level.<br>• 10: The tone volume is equal to the transmit audio level.<br>**Note:**<br>Avaya J129 IP Phone does not support this parameter. |

# 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.

### 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:<br>• 12125557722<br>• 1 212 555 7722<br>You can add spaces for readability.<br>Example:<br>`SET DIGIT_MAPPING "12125557722,12125557724"`<br>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:<br>• 8831 xxx xxxx |
| . | .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:<br>• 0011 64 x. |

*Table continues…*

| Element sign | Element name | Element description | Rule example |
|---|---|---|---|
| [ ] | 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:<br>• [^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:<br>• !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 (:).<br><br>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 (:).<br><br>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.<br>• <02:>xxxx xxxx - Take 02, replace it with nothing, then match the next 8 digits.<br>• <02>xxxx xxxx or <:02>xxxx xxxx - Add 02 to the start of an 8-digit number |

**Related links**

Digit mapping parameters on page 247

## 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.<br>Value operation:<br>• 0: Disabled<br>• 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.<br>Valid value is a string of alphanumeric rules. If a rule uses incorrect characters, the phone ignores it.<br>The preferred way of configuring this parameter is through the web interface. |

**Related links**

Digit mapping on page 244

# Enable access to restart the phone

Depending on the requirement, you can provide access to the user to restart the phone from the Login screen. If you enable access, the phone displays the Restart soft key on the Login screen for the user. Use the `46xxsettings.txt` file or the phone web interface to configure access for the end-user to restart the phone from the Login screen.

When you enable the access to reboot the phone, the phone logs indicate the reboots that the end-user initiate.

## Configuring parameter to enable the restart of the phone

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

| Parameter name | Default value | Description |
|---|---|---|
| RESTART_FROM_LOGIN | 0 | Specifies if the phone displays the Restart soft key from the Login screen. When the user presses the Restart soft key, the phone prompts to confirm the restart. Upon user confirmation, the phone restarts.<br>The options are:<br>• 0: Disable<br>• 1: Enable<br>**Note:**<br>Avaya J129 IP Phone does not support the restart of the phone from the Login screen. |

## Enabling access to restart the phone using the web interface

### About this task

Instead of plugging-out and plugging-in the Ethernet cable of the phone to restart the phone, the user can use the Restart soft key on the Login screen. You can enable access for the end-user to restart the phone from the SIP Login screen.

### Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Settings**.
3. In the Phone Menu Options area, scroll to **Restart from login**.
4. Choose **Enable** to display the Restart soft key on the SIP Login screen.

# Extension to Cellular

With the Extension to Cellular (EC500) feature, you can do the following:

- Receive an incoming call of your Avaya phone on your personal phone by using **EC500** button when you are away from your desk.
- Extend an ongoing call to your cell phone by using **Extend Call** button. When you answer the extended call on your cell phone, the call remains active on your office phone. Later you can switch back to your office phone to continue the call.

You must activate this feature by using Avaya Aura® Communication Manager.

# Exclusion

The Exclusion feature is used to prevent other multi-appearance users to bridge on to the same extension for an existing call.

You must activate this feature on the Avaya Aura® Communication Manager.

# Feature target selection

The users can enter the extension number manually or use target selection such as Contacts, Recents, or Phone buttons to select the extension number from the list. The user can also use autodial, busy indicator, or team line key to select the number as destination target.

To provide user access, enable the feature target selection using one of the following methods:

- `46xxsetting.txt` file
- Web interface of the phone

This feature applies to Call Forward, Call Forward-No Answer, Call Forward-Busy, Whisper Page, Priority, CPN Block, CPN Unblock, Transfer, Conference, and No Hold Conference.

## Configuring feature target selection using web interface

### About this task

Use this procedure to enable or disable the feature target selection for entering the destination number 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 **Feature target selection**, click one of the following:
   - **Enable**: To enable feature target selection.
   - **Disable**: To disable the feature target selection. It is a default option.

## Feature target selection parameters

Use the `46xxsettings.txt` file to set the following parameter for feature target selection:

| Parameter name | Default value | Description |
|---|---|---|

*Table continues…*

| | | |
|---|---|---|
| ENABLE_FEATURE_INVOCATION_TARGET_SELECTION | 0 | This parameter is used to enable or disable the feature target selection.<br>The options are:<br>• 0: Disabled. This feature is disabled by default. The user must manually enter the extension number.<br>• 1: Enabled. Enable the feature target selection. The user can enter the destination number using dial, contacts, recents, and phone buttons. The user can also use the browser soft key, autodial, busy indicator and team line keys to select the destination number. |

# 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 (=)

### 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.<br>The valid value is a string of up to 255 ASCII characters without any intervening spaces.<br>Double quotes (“”) must not be used in a username string when you configure this parameter through the `46xxsettings.txt` file.<br>The following symbols are not supported when provisioning the credentials with the DHCP Option 242:<br>• Double quote mark (“”)<br>• Apostrophe (’)<br>• Comma (,)<br>• Equal (=) |

*Table continues…*

| Name | Default value | Description |
|---|---|---|
| FORCE_HTTP_AUTH_PASSWORD | Null | Specifies the password for HTTP/HTTPS provisioning server authentication.<br>The valid value is a string of up to 255 ASCII characters without any intervening spaces.<br>Double quotes (“”) must not be used in password string when you configure this parameter through the `46xxsettings.txt` file.<br>The following symbols are not supported when provisioning the credentials with the DHCP Option 242:<br>• Double quote mark (“”)<br>• Apostrophe (’)<br>• Comma (,)<br>• Equal (=) |

# Guest login

With the Guest Login feature, a guest user can login to another end user’s primary phone and use the phone for a specific period.

## Guest Login configuration

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

| 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.<br>Valid values are integers from 1 to 12. |
| GUESTLOGINSTAT | 0 | Specifies whether the Guest Login feature is available to users.<br>Value Operation:<br>• 0: The feature is not available.<br>• 1: The feature is availble.. |

*Table continues…*

| Parameter name | Default Value | Description |
|---|---|---|
| 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.<br><br>Valid values are integers from 1 to 15. |

# Hunt Group Busy Position

With the Hunt Group Busy feature, end users can opt-in or opt-out of the calls specific to the hunt group. A hunt group is a collection of users who handle similar types of calls. A user can take part in multiple hunt groups.

The Hunt Group Busy feature must be configured on Avaya Aura® System Manager.

# Intercom

With the Intercom feature, the user can press the intercom feature button to call another user in a predefined intercom group. The Intercom feature offers Dial and Auto intercom features to make intercom calls.

With the Dial intercom feature, the user can dial extension codes to call anyone in the same intercom group. You must configure the intercom group and the digit codes for the required extensions.

With the Auto intercom feature, the user can call one predefined number in the same intercom group. You must configure the destination extension number.

The feature is not supported in Avaya J129 IP Phone for making an outgoing call. If you configure the Intercom feature for this phone, the user can accept an auto intercom incoming call.

Configure the intercom groups, the extension codes, and the destination extension number using Avaya Aura® Communication Manager R10.1 2 and later. For more information about the Intercom feature configuration, see Avaya Aura® Communication Manager Feature Description and Implementation on Avaya support site.

## Auto intercom feature settings

This section describes the behavior of the Auto intercom feature with the other active phone features. If Auto-answer all calls or Auto-answer intercom calls features are activated, the auto intercom call auto-answers on the phone. In this case, if the user wants to restrict the audio from their phone, you can enable the Auto-mute intercom call feature. The Auto-mute intercom call feature mutes the phone when it receives an auto intercom call with an active auto-answer. The user must manually unmute the call to establish two-way audio.

You can enable the Auto-mute intercom call feature in the Avaya Aura® Communication Manager R10.1.2 and later. For more information about the Auto intercom feature settings, see Avaya Aura® Communication Manager Feature Description and Implementation on Avaya support site.

# Long-term acoustic protection

Avaya J100 Series IP Phones support long-term acoustic exposure protection to prevent users from getting acoustic shocks. This feature reduces the loud volume of the conversations on the phone call to permissible acoustic limits. You and the phone user can set the acoustic limit value. If you set the acoustic limit value, that value is available to the user as a default value. If you do not set the acoustic limit value, the default value of the parameter ACOUSTIC_EXPOSURE_PROTECT_MODE_DEFAULT is the default value on the phone UI. The phone UI displays a list of permissible acoustic limit values and the default value for the user selection.

Long-term acoustic protection is supported only in L100 Series Headsets with an RJ9 connector and the Headset Profile1.To set the acoustic limit value use the phone web interface or the `46xxsettings.txt` file.

**Note:**

Avaya J129 IP Phone does not support long-term acoustic protection.

## 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.<br>The options are:<br>• 1: Off<br>• 2: Dynamic<br>• 3: 4 hours<br>• 4: 8 hours<br>If you set the value to Dynamic, the feature activates itself during loud phone conversations to gradually reduce the loud volume and prevent it from reaching damaging decibel levels.<br>**Note:**<br>Avaya J129 IP Phone does not support long-term acoustic exposure protection. |

# Limit Number of Concurrent Calls

The Limit Number of Concurrent Calls (LNCC) feature is used to control the number of concurrent incoming calls, and to change Multiple Call Appearance phone to a Single Call Appearance

phone. If a user is active on a call and receives an incoming call, if the **LimitInCalls** feature is enabled, the caller gets the busy tone.

This feature must be activated on the Avaya Aura® Communication Manager.

# 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.<br>Value operation:<br>• 0: No<br>• 1: Yes |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| DIRUSERNAME | Null | Specifies the LDAP client username.<br>The following characters are allowed:<br>• 0–9<br>• a-z<br>• A-Z<br>The preferred way of configuring this parameter is through the web interface. |
| DIRPASSWORD | Null | Specifies the LDAP client password.<br>The following characters are allowed:<br>• 0–9<br>• a-z<br>• A-Z<br>The preferred way of configuring this parameter is through the web interface. |
| DIRSRVR | Null | Specifies the IP address or a fully qualified domain name (FQDN) of the LDAP directory server.<br>The valid value is an IPv6 or IPv4 address in the dotted decimal format or a FQDN.<br>For example,<br>`SET DIRSRVR 192.168.161.54`<br>or<br>`SET DIRSRVR domain.com` |
| DIRSRVRPRT | 389 | Specifies the port number for the LDAP directory server.<br>Valid values are positive integers from 1 to 65535.<br>For example,<br>`SET DIRSRVRPRT 389` |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| DIRTOPDN | Null | Specifies the LDAP search base.<br>For example,<br>`SET DIRTOPDN "dc=global,dc=avaya,dc=com"` |
| DIRSECURE | 1 | Specifies whether to use TLS or TCP for the LDAP server.<br>Value operation:<br>• 0: Use TCP<br>• 1: Establish TLS connection using the STARTTLS extended operation.<br>• 2: Establish TLS connection using the Secure LDAP protocol (LDAPS)<br>For example,<br>`SET DIRSECURE 1`<br>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.<br>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.<br>Value operation:<br>• 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.<br>• 1: Simple LDAP Authentication and Security Layer (SASL).<br>If a connection is established over TLS (DIRSECURE is set to 1 or 2), DIGEST-MD5 or PLAIN authentication mechanisms are supported.<br>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.<br>When configuring the DIRSEARCH_FIELDS parameter, you must use attribute names that coincide with the selected LDAP server attribute names.<br>For example,<br>`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.<br><br>You can use this parameter to map the specified LDAP keywords. This mapping defines the way the phone displays the fields with LDAP details.<br><br>For example,<br><br>`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"`<br><br>In this example, the format is as follows:<br><br>`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.<br>The attributes specified in this parameter must be a subset of the attributes specified in DIRNAME_FIELDS.<br>For example,<br>`SET DIRNAME_FIELDS "cn,sn"`<br>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.<br>For example,<br>`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.<br>Local contact field names can be assigned from the following:<br>• "firstname"<br>• "nickname"<br>• "URI"<br>• "extension"<br>• "email"<br>• "department"<br>• "zipCode"<br>• "country"<br>for number types:<br>• "work"<br>• "home"<br>• "mobile"<br>• "other" |
| DIR_LDAP_DESCRIPTION | “LDAP Directory” | Specifies a custom label to be used for the LDAP directory in the Contacts application.<br>Valid value is a text string. |

# Multiple Device Access

Avaya J100 Series IP Phones support Multiple Device Access (MDA) with which you can simultaneously register up to 10 SIP devices for one user. You can define the Maximum Simultaneous Device using the Avaya Aura® System Manager.

With MDA, the user can do the following:

- Make and receive calls on any registered device.
- Move to another registered device during an active call.
- Bridge on to calls on multiple registered devices.

  Alert other registered devices about an incoming call to your extension. When user answers a call on a device, the alerts on all the other devices stop. During the call, the other devices display an active call indicator on the call appearance for the active line.

- Be on multiple concurrent calls on different devices, but only one call on each device.

  For example, user can listen to a conference call on one device and answer an incoming call on a second device without putting the conference call on hold. The two calls are on separate call appearances on all registered devices.

- Use conference and transfer features.

  When user bridges on to a call on any of the registered devices and start a transfer, the call drops from all devices after the transfer is complete.

If you try to register a new SIP device that exceeds the defined Maximum Simultaneous Device, then the user on the first registered device is logged out. You can define the behavior of the first registered device with the parameter PROVIDE_LOGOUT.

When you set PROVIDE_LOGOUT to 0, the device logs out and the phone screen does not show the login screen. However, the phone screen displays **Login** soft key for the user to login automatically without prompting for the credentials.

When you set PROVIDE_LOGOUT to 1, the device logs out and the phone screen displays the login screen. To enable the user to login without entering the credentials, use **Quick Login Status** in Avaya Aura® System Manager. For more information, see Avaya Aura® System Manager documentation.

For more information on the Multiple Device Access, see *Multi Device Access White Paper* on Avaya support site.

**Related links**

Multi-Device Access

## Multi Device Access operation in dual-stack mode

When the phone is configured in the IPv4 and IPv6 dual-stack mode with Multi Device Access (MDA) support, the signaling address family is selected according to the order of precedence level. The settings are done in both `46xxsettings.txt` file and System Manager. The order of precedence is as follows:

- Phone through Administration menu settings
- Web user interface
- Avaya Aura® System Manager
- Settings File
- DHCP
- LLDP

If you log in with your extension on MDA2 during a call and the signaling address mode is different from that of MDA1, then a limited service icon momentarily displays on MDA2. MDA2 automatically switches its signalling address family to match MDA1.

| Parameter | Description |
|---|---|
| SIP_CONTROLLER_LIST_2 | Describes the list of SIP Proxy or Registrar servers separated by comma when the SIP device is configured for the dual-stack operation.<br>Valid values are 0 to 255 characters in the dotted decimal or colon-hex format.<br>The syntax is:<br>`host[:port][;transport=xxx]`<br>where<br>• `host` is IP addresses in dotted-decimal format or hex format.<br>• `[:port]` is the port number. The default values are 5060 for TCP and 5061 for TLS.<br>• `[;transport=xxx]` is the transport type and `xxx` is either TLS or TCP. The default value is TLS.<br>For example, `SIP_CONTROLLER_LIST_2="10.16.26.88:5060;transport=tcp"` |
| SIGNALING_ADDR_MODE | Describes the SIP registration over IPv4 or IPv6 and selects the preferred Avaya Aura® Session Manager for phones supporting the dual-stack mode. The Avaya Aura® Session Manager IP address is selected according to the parameter SIP_CONTROLLER_LIST_2.<br>Valid values are:<br>• 4: IPv4. This is the default value.<br>• 6: IPv6 |

## Shared Control

With the Shared Control feature (SC), you can control phones using a soft phone client. Phones must be registered with Avaya Aura® to establish a shared control connection. The value of SIP_CONTROLLER_LIST must be identical in both phones and should have same configuration. A shared control session might not be established if multiple devices are registered to the same user with the SC-enabled flag sent during registration, depending on the soft client implementation.

**Note:**

- SIP signaling must be set to TLS for the phone and the soft client. For security reasons, TCP is not supported with Shared Control.
- Avaya J100 Series IP Phones now supports the Shared Control feature on all phone models.

# Multiple Level Precedence and Preemption

You can override other calls by making a priority call with precedence. You can manually dial the extension number or select the extension from the Contacts or the Recents lists. The precedence level is valid for only one call session. The available call precedence levels are:

- FO: Flash Override. Highest precedence
- FL: Flash
- IM: Immediate
- PR: Priority
- Routine: Lowest precedence. Routine is highlighted on the call session line if no call is made within five minutes.

**Note:**

You can start a precedence call from Busy Indicator and Bridged Appearance but not from the Team button.

This feature must be activated on the Avaya Aura® Communication Manager.

## MLPP configuration

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

| Parameter name | Default value | Description |
|---|---|---|
| DSCPAUD_FL | 43 | Specifies the DSCP value for flash precedence or priority level voice call.<br>Valid values are from 0 to 63. |
| DSCPAUD_FO | 41 | Specifies the DSCP value for flash Override precedence or priority level voice call.<br>Valid values are from 0 to 63. |
| DSCPAUD_IM | 45 | Specifies the DSCP value for immediate precedence or priority level voice call.<br>Valid values are from 0 to 63. |
| DSCPAUD_PR | 47 | Specifies the DSCP value for priority precedence or priority level voice call.<br>Valid values are from 0 to 63. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ENABLE_PRECEDENCE_SOFT KEY | 1 | Specifies that whether the precedence soft key is enabled or not on the idle line appearances on Phone Screen.<br>Value Operation:<br>• 0: Disabled.<br>• 1: Enabled. |
| ENABLE_MLPP | 0 | Specifies that whether the Multiple Level Precedence and Preemption (MLPP) is enabled or not.<br>Value Operation:<br>• 0: Disabled.<br>• 1: Enabled. |
| MLPP_MAX_PREC_LEVEL | 1 | Specifies the maximum allowed precedence level for the user.<br>Value Operation:<br>• 1: Routine<br>• 2: Priority<br>• 3: Immediate<br>• 4: Flash<br>• 5: Flash Override |
| MLPP_NET_DOMAIN | Null | Specifies the MLPP network domain.<br>Value Operation:<br>• Null: No domain configured<br>• DSN: DSN network.<br>• UC: UC network. |
| DSCPMGMT | 16 | Specifies the DSCP value for OA&M management packet.<br>Valid values are from 0 to 63.<br>**Note:**<br>Only Avaya J129 IP Phone supports this feature. |

# 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 not supported in the IP Office environment in CCMS mode.

**Related links**

Configuring Multicast Paging on page 197
Multicast Paging configuration on page 268

## 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.<br>This is the basic parameter for this feature. If this parameter is not set, other parameters listed below will be ignored.<br>Valid values:<br>• 0: Multicast Paging is disabled.<br>• 1: Multicast Paging is enabled. |
| 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.<br>The paging groups should be separated with a comma (“,”), and should be listed in the following format:<br>`IP:port:priority:label`<br>where<br>• `IP` is the multicast IP address of an MP group;<br>• `Port` is the IP port of a Multicast Paging group, the valid value is an even integer ranging from 1024 to 65534;<br>• `Priority` is the priority of a group. Allowed values are 1 through 16, with smaller values indicating a higher priority;<br>• `Label` is a group label which is displayed in notification messages when the incoming page from this group is played.<br>All the above-listed settings are required.<br>For example,<br>`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.<br>The paging groups should be separated with a comma (“,”), and should be listed in the following format:<br>`IP:port:label`<br>`IP`, `Port`, and `Label` denote the same as the corresponding MP_GROUPS_TO_LISTEN values. All these settings are required.<br>For example,<br>`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.<br>Valid values:<br>• 1: G.729 codec is used.<br>• 2: G.711u codec is used.<br>• 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.<br>The value must be valid for the selected codec and therefore must not be changed unless necessary. |

# Malicious call tracing

With the Malicious Call Tracing feature, the end user can track a malicious or threatening call. Activating Malicious Call Tracing (MCT Act) alerts a controller to begin call tracing and provide information for reporting this call. The administrator must set up the phone system to trace and track malicious calls and there should be an attendant or controlling user to oversee the trace.

This feature must be activated on the Avaya Aura® Communication Manager.

# No Hold Conference

The No Hold Conference (NHC) feature allows a user to set up a conference call without interrupting the current conversation.

For example, if you press the administered **No Hold Conf** feature button and then dial an extension the participant that answers the call joins the no hold conference.

If an extension number is pre-configured on SMGR, and you press the **No Hold Conf** feature button the call is placed to the pre-configured number when the participant answers the call joins the no hold conference.

Using the **No Hold Conf** feature button you can add more participants to the no hold conference.

If the participants do not answer the call within a prescribed time limit, Avaya J100 Series IP Phones will display an error on the phone screen.

You can activate this feature on Avaya Aura® Communication Manager.

**Note:**

You can pre-configure only one extension number on SMGR for no hold conference.

### No hold conference limitation

In order to correctly use the No hold conference feature, make sure that CONFERENCE_FACTORY_URI value is null. The phone does not support No hold conference and CONFERENCE_FACTORY_URI simultaneously.

# Night mode

With the Night mode feature, the users can dim the light of the phone screen to minimum. Use the Settings file or the phone web interface to enable and disable the Night mode feature. When you enable the feature, the phone idle screen, Login screen, and the Brightness settings screen displays the Night mode menu option. Additionally, you can configure the Night mode soft key for an idle call appearance line.

When the user activates the Night mode feature, the phone switches off the Beacon LED, the Missed call LED, and the Red LED on the line keys. The phone continues to display the green LED on the line keys for the other active features.

The Night mode feature does not affect the illumination of the Speaker, Mute, and Headset buttons.

**Note:**

The Night mode screen is dimmer than the standard brightness of the phone.

Only Avaya J179 IP Phone supports this feature.

**Related links**

Soft key configuration on page 217

## Configuring Night mode using the phone web interface

### About this task

Use this procedure to enable or disable the Night mode 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 **Brightness**.
4. In **Night Mode Softkey**, click one of the following:
   - **Do Not Allow (Default)**: To disable the night mode feature. The phone UI does not display the Night soft key.
   - **Allow**: To enable the Night mode feature. The phone UI displays the Night soft key.

## Night mode configuration

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

| Parameter name | Default Value | Description |
|---|---|---|
| ENABLE_NIGHT_MODE | 0 | Specifies whether the Night mode soft key is available on the phone UI.<br>The options are:<br>• 0: Do not allow<br>• 1: Allow |

# 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<br>Value operation:<br>• 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.<br>Value operation:<br>• "": Disabled<br>• An extension number: The phone dials this number in case of an off-hook alert event. |

# Presence

With the Presence feature, an end user can view the status of contacts in real time. End user can also change his own presence status according to his availability.

## Configuring Presence by using the web interface

### About this task

Use this procedure to enable or disable complete presence options.

### Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **Settings**.
3. Click **Feature access**.
4. In the **Presence** field, click one of the following option:
   - **Allow**: To enable the presence options.
   - **Do not allow**: To disable the presence options.

## Presence configuration

You must activate this feature on Avaya Aura® Communication Manager.

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

| Parameter name | Default Value | Description |
|---|---|---|
| ENABLE_PRESENCE | 1 | Specifies whether presence is supported.<br>The options are:<br>• 0: Disabled<br>• 1: Enabled<br>**Note:**<br>This parameter is set to 0 in an IP Office and Open SIP environment. |
| ALLOW_DND_SAC_LINK_CHANGE | 0 | Specifies if the user is allowed to change the DND and SAC button link. If the change is allowed, the menu to set the DND and SAC link is displayed.<br>The options are:<br>• 0: Do not allow a user to change default behavior (Default)<br>• 1: Allow a user to change the default behavior<br>**Important:**<br>This parameter is not supported from firmware version 4.0.8.0 and later. Starting from firmware version 4.0.8.0, the parameter DND_SAC_LINK provides the enhanced functionality. |
| AWAY_TIMER | 1 | Controls whether the phone reports an away state.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled (default). The phone automatically reports an away state |

*Table continues…*

| Parameter name | Default Value | Description |
|---|---|---|
| AWAY_TIMER_VALUE | 30 | Specifies the idle time duration, after which the phone assumes that the user is away from the phone.<br>The range is 1-1500 minutes. |
| DND_SAC_LINK | 0 | Specifies whether to activate the Send all call when the user enables Do not disturb.<br>The value of this parameter is used if the ALLOW_DND_SAC_LINK_CHANGE is set to 0<br>Value operation:<br>• 0: Do not activate the Send all call when the user enables Do not disturb (default)<br>• 1: Activate the Send all call when the user enables Do not disturb<br>• 2: Activate the Send all call when the user enables Do not disturb and vice-versa<br>• 3: Forced do not activate the Send all call when the user enables Do not disturb<br>• 4: Forced activate the Send all call when the user enables Do not disturb<br>• 5: Forced activate the Send all call when the user enables Do not disturb and vice-versa<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |

*Table continues…*

| Parameter name | Default Value | Description |
|---|---|---|
| PRESENCE_ACL_CONFIRM | 0 | Specifies the handling of a Presence ACL update with pending watchers.<br>The options are:<br>• 0: Auto confirm. Automatically send a PUBLISH to allow presence monitoring. This is the default value<br>• 1: Ignore.— Take no action<br>This parameter is not supported in an IP Office environment. |

# 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.<br>Valid value is a string of correct codec names, separated by a comma with no blank spaces. For example:<br>`SET CODEC_PRIORITY OPUS,G722,G711U,G711A,G726, G729`<br>If values are entered incorrectly or the phone does not support the listed codec, the value is ignored. |

# Priority Calling

With the Priority Calling feature, users can signal a busy internal extension that a call needs immediate attention. Priority calls have a distinctive ring. Users can make a priority call to an extension that is set to **Do not disturb**. If an extension is configured for call forwarding, priority calls retain their priority until a user answers.

You must activate Priority Calling on Avaya Aura® Communication Manager.

## Priority Calling configuration

Set the following parameter in the `46xxsettings` file:

| Parameter name | Default value | Description |
|---|---|---|
| RINGPRIORITY | 3 | Specifies the distinctive ring rate for a priority call.<br>Valid values:<br>• 1: Internal call rate.<br>• 2: External call rate.<br>• 3: Priority call rate. |

# Push

The Push feature enables trusted applications to send content to Avaya J100 Series IP Phones without user input.

The Push process is a two-step operation that consists of the following:

- Push request to the phone. The Push Initiator server application transmits a Push request using an HTTP POST method to the Push Agent phone application.
- Pull request to the trusted server. The Push Agent requests the URI of the content from a trusted Push server.

The Push content is a WML file for the WML browser or an XML file for setting up an RTP audio stream, displaying a message on the Top line, or other broadcasts.

The requested Push content can be the following:

- `audio`: Phone receives or transmits a non-call unicast RTP audio stream. Push content message specifies the receive or the transmit type.
- `display`: Phone downloads and renders a WML file in the browser.
- `receive`: Phone receives a non-call unicast RTP audio stream.
- `subscribe`: Phone sends a Subscribe message to the server.
- `top line`: Phone downloads an `.xml` file that contains the text to display on the top line.
- `transmit`: Phone transmits a non-call unicast RTP audio stream.
- `multicast`: Phone receives a non-call multicast RTP audio stream.
- `phonexml`: Phone downloads a `.phonexml` file.

The Push requests have two priorities, normal and barge-in. The priorities correspond to the two Push modes, Normal and Barge.

## Secure Push

Using the Secure Push feature, trusted applications can transmit data to the Avaya J100 Series IP Phones over a secure connection.

Secure Push uses the HTTPS protocol for incoming and outgoing requests to the phone. The URI of the secure Push uses the DNS name instead of the IP address for hostname validation.

The initial `subscribe` message sent to the server indicates whether the phone supports secure or non-secure Push.

The administrator must enable the PUSH_MODE parameters in the settings file to secure and non-secure Push connections.

**Note:**

You must install the Push Servers identity certificates on the phone for a secure Push connection. If the identity certificate is not installed, the applications ignore the `push mode` setting and use HTTP.

## Push configuration

Set the following parameters in the `46xxsettings.txt` file to configure the Push feature:

| Parameter name | Default value | Description |
|---|---|---|
| PUSHCAP | 00000 | Specifies the Push type modes that the phone supports.<br>The Push value is a 3, 4, or 5-digit number. Each digit controls a specific Push type:<br>• 0: Reject all Push requests.<br>• 1: Accept the Barge mode Push requests.<br>• 2: Accept the Push requests for Barge or Normal modes.<br>For example, for a PUSHCAP value of `21202`:<br>• 2: Controls phonexml Push requests.<br>• 1: Controls audio-transmit Push requests.<br>• 2: Controls audio-receive Push requests.<br>• 0: Controls display Push requests.<br>• 2: Controls top-line Push requests.<br>**Note:**<br>Avaya J129 IP Phones and Avaya J139 IP Phones do not support display Push WML browser requests. |
| PUSHPORT | 80 | Specifies the TCP port number of the HTTP server for the Push requests.<br>Valid value is a positive integer between 80-65535. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| TPSLIST | Null | Specifies a list of URI authority components to obtain the Push content. The list supports HTTPS and HTTP.<br>Valid values can contain up to 255 characters and must be comma-separated without intervening spaces.<br>**Note:**<br>If you set TPSLIST to default, the Push feature is disabled. |
| SUBSCRIBELIST | Null | Specifies a list of URIs to which the phone sends 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 request for the URI with the phone MAC address, extension number, IP address, and model number appended as query values.<br>The list can contain up to 255 characters. Values are comma-separated without intervening spaces.<br>If you set the value to null, subscribe messages are not sent. |
| PUSH_MODE | 2 | Specifies the combination of secure and non-secure Push.<br>Valid values:<br>• 0: Enables non-secure Push.<br>• 1: Enables secure Push.<br>• 2: Enables secure and non-secure Push.<br>**Note:**<br>If PUSH_MODE= 2 (Both), applications send subscribe requests using secure Push. If secure Push fails, subscribe requests are sent over a non-secure connection. |
| PUSHPORT_SECURE | 8443 | Specifies the listening port for the secure Push request. Secure push uses HTTPS. |

# Ringtones

The Avaya J100 Series IP Phones have eighteen ringtones by default. You can add ringtones using the RINGTONES parameter in `46xxsettings.txt` text file. It specifies a list of audio files to download as ring tones and offer to users for selection.

You can also personalize the ringtones option on the phone for the users. The phone saves the user selections in the Personal Profile Manager (PPM).

## Downloadable ringtones

You can specify list of audio files that phones can download as ringtones. The users can select the required ringtone from the downloaded list.

The audio files list can contain 0 to 1023 UTF-8 characters. Provide the list of audio files as name-value pairs separated by commas without any intervening spaces, where:

- name: It is the display name that you assign to the ringtone. Ensure that you:
  - Do not include a comma, an equals sign (=), or a double quote character in the display names.
  - Quote the entire list if you include spaces in any of the display name.
  - Specify the display name that has the length that your deskphone can display. If the length of the display name exceeds the specified limit of your deskphone, the deskphone truncates the name.
  - Do not specify a display name that contains only numbers.
- value: Is the relative or an absolute URL of the audio file. URLs can include an equals sign (=). If you include the equals sign, the system treats the first equals sign as the separator between the display name and the URL. The system treats any subsequent equals signs after the first sign as a part of the URL. Percent encode a comma if you use it in the URL.

Ensure that audio files must:

- Be single-channel WAV files.
- Have encoding as per ITU-T G.711 A-law or u-law PCM with 8-bit samples at 8 kHz or 16-bit samples at 16 kHz.
- Have a maximum size of 512 KB.
- Have a combined size of not more than 5 MB.
- Only contain ASCII characters in their file names.

For example,

```
SET RINGTONES "Steam Whistle=tones/swhistle.wav,Car Horn=tones/chorn.wav,Loud
Burp=tones/lburp.wav"
```

## Ringtone Parameters

Use the `46xxsettings.txt` to set the following parameters for ringtones.

| Parameter name | Default Value | Description |
|---|---|---|
| RINGTONES | Null | Specifies a list of display names and file names or URLs for a custom ring tone files to download and offer to users.<br>The list can contain 0 to 1023 UTF-8 characters. The default value is null.<br>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. |
| 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.<br>Value operation:<br>• 0: Phone only tries to download ring tones with new display names.<br>• 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**.<br>Value operation:<br>• 0: North American ring tones are offered (default).<br>• 1: European ring tones are offered. |
| PROVIDE_CF_RINGTONE | 0 | Specifies if the call forward ringtone option is provided to the user.<br>Value operation:<br>• 0: The call forward ringtone option is not provided (default).<br>• 1: The call forward ringtone option is provided. |

*Table continues…*

| Parameter name | Default Value | Description |
|---|---|---|
| PROVIDE_PRIMARY_RINGTONE | 1 | Specifies if the user menus related to the ringtones are displayed on the phone user interface and the web interface.<br>Value operation:<br>• 0: The user menus are not displayed<br>• 1: The user menus are displayed |
| 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_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. |

# 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.<br>Value operation:<br>• 0: Line scrolling mode is used.<br>• 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.

# Send All Calls

The Send All Calls (SAC) feature redirects incoming calls to a predefined coverage number. You can enable the feature on Avaya Aura® Communication Manager and assign a number to redirect calls. When the feature is active, all incoming calls ring once at the user extension before being routed to the assigned number. By default, the phone screen displays the label of this feature as **Do not disturb**. You can use Avaya Aura® System Manager. You can use the parameter DND_SAC_LINK to define the relation between Send All Calls and DND presence status.

The SAC icon is similar to the presence-state DND icon. As an administrator, you can define an alternate icon ( ) for the SAC feature. When you enable the SAC feature, an alternate icon displays on the phone screen. Use one of the following methods to configure the SAC icon:

- 46xxsetting.txt file
- Web interface of the phone

### Related links

Presence configuration on page 273

## Configuring the SAC icon using the web interface

### Procedure

1. Log in to the web interface.
2. In the navigation pane, go to **Settings**.
3. Select **Feature access**.
4. In the **SAC feature icon**, click one of the following:
   - **DND style (Default)**: With this option, you can use the SAC icon, which is similar to the presence-state DnD icon.
   - **SAC style**: With this option, you can use to use a different SAC icon.

## Parameter for configuring the SAC icon

Use the `46xxsettings` file to set the following parameter:

| Parameter name | Default value | Description |
|---|---|---|
| SAC_ICON | 0 | This parameter is used to define the icon for the SAC feature.<br>Value operation:<br>• 0 (Default): Use the SAC icon similar to the presence-state DnD icon.<br>• 1: Use an alternate SAC icon.<br>**Note:**<br>Avaya J129 IP Phone does not support this parameter. |

# Service Observe

In the Avaya Aura® Call Center Elite environment, a supervisor can use the Service Observe feature to perform the following actions:

- Monitoring a phone call to observe the call quality.
- Talking to the agent and the customer.
- Coaching the agent during call observation.

In the Unified Communications Module environment, a supervisor can use the Service Observe feature to perform the following actions:

- Monitoring a phone call to observe the call quality.
- Talking to the agent and the customer.

Service Observe is available on Avaya J169, J179, and J189 IP Phones.

You can use Avaya Aura® System Manager to configure Service Observe. For more information about how to configure the feature, see the Avaya Aura® System Manager documentation.

Use the Computer Telephony Integration (CTI) client to activate or deactivate Service Observe on the phone remotely. For more information about how to use CTI, see the Avaya Aura® Application Enablement Services documentation.

If you use the Service Observe feature through CTI, you must set CC_INFO_TIMER to 0.

# Server-initiated update

With the Server-initiated update feature, you can get a notification from the SIP server when there is a new software or file available on the file server. The Server-initiated update feature is disabled by default. To enable this feature, you must set the ENABLE_OOD_RESET_NOTIFY parameter to 1.

When the phone receives a SIP NOTIFY message about available updates, the phone compares the firmware version in the `J100Supgrade.txt` file on the file server with the current version installed. If the file server has the latest firmware, the phone reboots and upgrades.

If there is an updated settings file on the server, the phone downloads the files to apply the new settings. Depending on the parameters that change, the phone logs out the current user or reboots. If there are active calls or other transmissions, the phones apply the new settings when the status is idle.

The Status tab in the web interface displays the date and time of the last update.

You can use either of the following to get the notification from the SIP server:

- the Administration menu on the phone
- the Management tab in the web interface

**Related links**

Updating phone settings and firmware on page 113
Management settings field descriptions on page 176
Status field description on page 121

# 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.<br>Valid values:<br>• 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.<br>• 1 - Enable (default). When a call on the selected line is ended, the highlighted line is not changed. |

# Team Button

The Team Button feature is used to:

- Monitor the status of the extensions of other team members.
- View the call redirection of the monitored phones.
- Answer any incoming call to the monitored station.
- Speed dial to call a monitored station that is idle.
- Override the call redirection feature that includes SAC, CFWD, or ECF to ensure that a call rings on the monitored phone.

To override call redirection, you must configure the monitored phone on Avaya Aura® System Manager.

For more information about setting the overriding permission, see *Administering Avaya Aura® System Manager*.

## Team Button configuration

This feature must be activated on the Avaya Aura® Communication Manager.

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

| Parameter name | Default Value | Description |
|---|---|---|
| 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.<br>Value Operation:<br>• 0: Disabled. The redirect indication is shown only on a monitoring station which is redirection destination.<br>• 1: Enabled. The redirection indication is displayed on all monitoring stations.<br>**Note:**<br>Avaya J139 IP Phone does not support this feature. |
| TEAM_BUTTON_RING_TYPE | 1 | Specifies the alerting pattern to use for team buttons.<br>Valid values are 1 through 8. The default value is 1.<br>**Note:**<br>Avaya J139 IP Phone does not support Team Button feature. |

# 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.

**Note:**

IP Office does not support this feature in CCMS mode.

## 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.<br>Value operation:<br>• 0: Disabled<br>• 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.

**Note:**

IP Office does not support this feature in CCMS mode.

## 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.<br>This parameter ignores the other values if the value is set to 1 (enabled by default).<br>Value operations:<br>• 0: Disabled<br>• 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.

**Note:**

IP Office does not support this feature in CCMS mode.

## 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.<br>This parameter ignores the other values if the value is set to 1 (enabled by default).<br>Value operations:<br>• 0: Disabled<br>• 1: Enabled |

**Note:**

This parameter is applicable only if USBPOWER value is not 0 (a default value).

# 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 MSGNUM parameter in `46xxsettings.txt` file to configure the voicemail number. When there is a failover from Avaya Aura environment to non-Avaya server, use PSTN_VM_NUM parameter to configure the voicemail number.

Refer to Avaya Aura® System Manager for specifying the voicemail number in the corresponding field before installing the phone.

**Note:**

If you set two different values for the same parameter through Personal Profile Manager (PPM) and the `46xxsettings.txt` file, the PPM settings override the settings in the `46xxsettings.txt` file.

## 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.<br>The features are defined as follows:<br>• 0 = Redial<br>• 1 = Contacts<br>• 2 = Emergency<br>• 3 = Recents<br>• 4 = Voicemail<br>**Note:**<br>Emergency calls are not supported in an Open SIP environment. |
| MSGNUM | Null | Specifies the phone number to be dialed automatically when the user presses the Message button. The phone number connects to the user's voice mail system.<br>**Note:**<br>This parameter is applicable in the Avaya Aura environment. In case of IP Office and third-party environment, use the parameter PSTN_VM_NUM. |

# 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 513
WML syntax specifications for Avaya J100 Series IP Phones on page 515

## WML browser limitation

When you set up a WML page, you must avoid mixing Postfield elements with URL query arguments. Otherwise the phone does not display Postfield values on the WML page.

See WML syntax specifications for Avaya J100 Series IP Phones on page 515 for WML syntax details.

## 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.<br>The allowed value contains not more than one URL of up to 255 characters.<br>**Note:**<br>If the value is set to default, the WML browser is disabled. |
| 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.<br>The allowed value must contain not more than one URL of up to 255 characters. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| WMLIDLETIME | 10 | Specifies the idle time in minutes, after which the web page set as the value of WMLIDLEURI is displayed.<br><br>The allowed value is a positive integer from 1 to 999.<br><br>**Note:**<br><br>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.<br><br>Allowed values are from 0 to 65535. |
| WMLPROXY | Null | Specifies the address of an HTTP proxy server that the WML browser uses.<br><br>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.<br><br>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.<br>Value operation:<br>• 0: The WML browser closes when the phone starts ringing and the phone displays an incoming call pop-up message.<br>• 1: The WML browser remains open, and the user can pick up the incoming call by off-hook from a WBL browser application. |

# Whisper Page

With the Whisper Page feature, the user can make an announcement to a person who is active on a call with the other members having the same extension. Only the person who is paged can hear the announcement.

This feature must be activated on the Avaya Aura® Communication Manager.

# Chapter 8: Avaya J100 Expansion module

## Expansion modules

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

Avaya J169/J179 IP Phones supports the JBM24 Button Module and Avaya J100 Expansion Module. Avaya J189 IP Phone supports only Avaya J100 Expansion Module.

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/ Applications | 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 |

*Table continues…*

| Power adapters | USB power | 1 JEM24 modules | 2 JEM24 modules |
|---|---|---|---|
| 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 |
| Avaya 5V DC 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, set the POE side switch to the H position. Alternatively, use the Avaya 5V DC power 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.

# JEM24 background and screen saver image configuration

You can set the screen saver and background image for Avaya J100 Expansion Module (JEM24) using the `46xxsettings.txt` file and the phone web interface.

You can choose the image from the available built-in images or upload custom images using the parameter **BACKGROUND_IMAGE_JEM**.

Depending on the requirement, if you provide access, the end user can also set the screen saver and background image of their choice for the JEM24 from the phone UI. Or, you can make settings such that the Primary screen and the JEM24 displays the same image. The JEM24 display reflects any changes made to the primary display.

You can configure access for the user to set the background and screen saver image using the `46xxsettings.txt` file and the phone web interface.

**Note:**

The user cannot set a background and screen saver image for the Avaya J100 Expansion Module, when you import new custom images. During this, the phone and Avaya J100 Expansion Module sync the images.

Avaya J100 Expansion Module does not support adjusting the display contrast.

# Import background and screen saver images of JEM24

You can add the background and screen saver images to the phone using `46xxsettings.txt` file.

Avaya J100 Expansion Module supports up to 5 custom background images.

Avaya J100 Expansion Module module only supports .jpg files with a maximum file size of 256 KB. The color depth is limited to 16 bits and the file names are case sensitive.

The Avaya J100 Expansion Module has a resolution of 272 x 480 pixels. You must store the image files in the directory specified by HTTPDIR or TLSDIR.

# JEM24 background and screen saver image configuration parameters

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

| Parameter Name | Default value | Description |
|---|---|---|
| BACKGROUND_IMAGE_JEM_FOLLOW_PRIMARY | 1 | Specifies whether the Avaya J100 Expansion Module background image always follows the primary display or can have a separate background image.<br>The options are:<br>• 0: You can configure a separate background image for the Avaya J100 Expansion Module background.<br>• 1: Avaya J100 Expansion Module background image always follows the primary display. |

*Table continues…*

| Parameter Name | Default value | Description |
|---|---|---|
| BACKGROUND_IMAGE_JEM | Null | Specifies a comma-separated list of custom background images for the Avaya J100 Expansion Module display.<br>The value is separated by commas without any intervening spaces.<br>Avaya J100 Expansion Module supports up to 5 background images with the following limitation:<br>• Only jpg format files are supported.<br>• The maximum file size is 256 KB.<br>• The file names are case sensitive.<br>• The color depth is limited to 16 bits.<br>The Avaya J100 Expansion Module has a resolution of 272 x 480 pixels.<br>The files must be stored in the directory specified by HTTPDIR or TLSDIR. |
| BACKGROUND_IMAGE_DISPLAY_JEM | 0 | Specifies the background image to be displayed on the Avaya J100 Expansion Module.<br>The default value is empty. The value is separated by commas without any intervening spaces.<br>To select one of the seven built-in default images, need to specify a value from 0 to 6.<br>• 0: Default image 1<br>• 6: Default image 7.<br>**Note:**<br>Note: If the parameter is not set, the phone sets the default Avaya device image as the Avaya J100 Expansion Module background image. |

*Table continues…*

| Parameter Name | Default value | Description |
|---|---|---|
| BACKGROUND_IMAGE_SELECTABLE_JEM | Null | Specifies whether the user can select a background image.<br>The options are:<br>• 0: The end user is not allowed to choose the Avaya J100 Expansion Module background image. The value set by an administrator is used.<br>• 1: The end user is allowed to choose the Avaya J100 Expansion Module background image. |
| SCREENSAVER_IMAGE_JEM_FOLLOW_PRIMARY | 1 | Specifies whether the Avaya J100 Expansion Module screen saver image always follows the primary display or can have a separate screen saver image.<br>The options are:<br>• 0: You can configure a separate screen saver image for the Avaya J100 Expansion Module screen saver.<br>• 1: Avaya J100 Expansion Module screen saver image always follows the primary display. |
| SCREENSAVER_IMAGE_JEM | Null | Specifies a comma-separated list of screen saver images for the Avaya J100 Expansion Module display.<br>Avaya J100 Expansion Module supports up to 5 screen saver images with the following limitation:<br>• Only jpg format files are supported.<br>• The maximum file size is 256 KB.<br>• The file names are case sensitive.<br>• The color depth is limited to 16 bits.<br>The Avaya J100 Expansion Module has a resolution of 272 x 480 pixels.<br>The files must be stored in the directory specified by HTTPDIR or TLSDIR. |

*Table continues…*

| Parameter Name | Default value | Description |
|---|---|---|
| SCREENSAVER_IMAGE_DISPLAY_JEM | 0 | Specifies the screen saver image to be displayed on the Avaya J100 Expansion Module.<br>The value is separated by commas without any intervening spaces.<br>To select one of the seven built-in default images, need to specify a value from 0 to 6.<br>• 0: Default image 1<br>• 6: Default image 7<br>**Note:**<br>Note: If the parameter is not set, then a Avaya J100 Expansion Module screen saver image must be set to default Avaya device image. |
| SCREENSAVER_IMAGE_SELECTABLE_JEM | Null | Specifies whether the user can select a screen saver image.<br>The options are:<br>• 0: The end user is not allowed to choose the Avaya J100 Expansion Module screen saver image. The value set by an administrator is used.<br>• 1: The end user is allowed to choose the Avaya J100 Expansion Module screen saver image. |

# Configuring JEM24 background and screen saver images by using web interface

## About this task

Use the web interface of the phone to configure the Avaya J100 Expansion Module background and screen saver images.

## Procedure

1. Log in to the web interface.
2. In the navigation pane, click **Background and Screen Saver**.
3. In the Background and Screen Saver area, configure the required parameters.
4. Click **Save** to save the setting.

# 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.

**Related links**

Downloading and saving the software on page 39
Upgrading the expansion module on page 302

# 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.

**Related links**

Downloading and saving the software on page 39
Avaya J100 Expansion Module upgrade on page 302

# Chapter 9: Security

## Security overview

SIP-based Avaya J100 Series IP Phones provide several security features. The phone lock and user logout functionalities protect the user's privacy. When the phone is locked, a user can only receive calls or make emergency calls. User logs and data are protected with the user account.

You can configure the following security features on the phones:

- Account management:
  - Storage of passwords and user credentials using Federal Information Processing Standards (FIPS 140–2).
  - FIPS 140-2 cryptographic algorithms for application, processes, and users.
  - Control to toggle between FIPS and non-FIPS modes.
  - Identity certificate installation using Simple Certificate Enrollment Protocol (SCEP) for enrollment and encrypted PKCS#12 file format to import private key and certificate.
- Certificate management:
  - X509v3 compliant certificates.
  - Public Key Infrastructure (PKI) for users who use third-party certificates for all Avaya services, including databases.
  - Support ECC and RSA (2048 and 4096 bit) keys for certificates in the certificate trust store and received from servers during TLS connections.
  - Support ECC and RSA (2048 bit only) keys for installed identity certificates.
  - Online Certificate Status Protocol (OCSP) for obtaining the revocation status of an X.509 digital certificate according to RFC 6960.
- Department of Defense solution deployment with Joint Inter-operability Test Command (JITC) compliance.
- VLAN separation mode using system parameters.
- Synchronization of the system clock at configured intervals using system parameters.
- Display of SSH fingerprint in the Administration menu.
- Display of OpenSSH and OpenSSL versions in the Administration menu.
- Maintenance of integrity when the phone is under Denial of Service (DoS) attack. In this case, the phone goes into out-of-service mode.

- DRBG random number generator compliant with SSL FIPS 140–2.
- SHA2 hash algorithm and strong encryption (AES-256 bit) for all cryptographic operations.
- Deprecated support for SHA1 algorithms in all cryptographic algorithms.
- SRTP/SRTCP and TLS v1.2.

  SRTP is used to encrypt and secure the audio going to and from the phone. You must configure equivalent parameters in Communication Manager or System Manager. You must configure the following three parameters on the phones, and equivalent Communication Manager parameters must match one of the parameters:

  - SET ENFORCE_SIPS_URI 1
  - SET SDPCAPNEG 1
  - SET MEDIAENCRYPTION X1, X2, 9. Valid values for X are 1 to 8 for aescm128-hmac80, and 10 or 11 for aescm256-hmac80

**Note:**

- The Administration menu provides access to specific administrative procedures on the phone. You must change the default password for the Administration menu to restrict users from using the administrative procedures to change the phone configuration.
- Remote access to the phone is completely disabled by default.
- You should not use unauthenticated media encryption (SRTP) files.

# 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.<br>Value operation:<br>• 0: Phone will not lock automatically.<br>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.<br>The value can be only digits, ranging between 4–20 characters.<br>if you do not set any value here, the SIP password can be used for unlocking the phone. |
| 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.<br>Value operation:<br>• 0: Disabled. **Lock** soft key and feature button are not displayed.<br>• 1: Enabled. **Lock** soft key and feature button are displayed. |

*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.<br>The value ranges between 5–1440 minutes. |

# Access control and security

Avaya J100 Series IP Phones provide the following security features for control and access:

### Security event logging

The phone maintains the Logs for the following events:

- Successful and failed logins, username lockouts, 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 and PEM file formats. The phone sends the device identity certificate and a private key along with the encrypted password to the WPA supplicant. The phone sends the EAP-MD5 password to the WPA supplicant 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 to see the IP information on the phone screen.

Use the parameter PROVIDE_NETWORKINFO_SCREEN to control the display of IP information.

### OpenSSH/OpenSSL version

The phone displays the version of OpenSSL and OpenSSH on the VIEW screen in the Administration menu when you set the parameter DISPLAY_SSL_VERSION to `1`.

### SSH Fingerprint

The phone displays SSH fingerprint to manually verify that a SSH connection is established with the correct phone.

### Time synchronization

The phone synchronizes the time with the configured NTP servers at intervals. The parameter SNTP_SYNC_INTERVAL checks the time interval for synchronization any time between 60 to 2880 minutes with 1440 as the default setting.

- Default: 1440 minutes
- 60–2880 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

## 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. You can view these logs for possible debugging issues related to installing and using certificates.

MIB object tables and IDs are created for certificates installed on the phone. You can view the certificate attributes through an SNMP MIB browser. MIB browser also provides you with the information of the configured certificates on the phone.

To implement DES, the phone has 64 Public CA certificates built-in. For a list of the certificates, see Public CA Certificates on page 530.

# Phone 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
```

**Note:**

If both MYCERTURL and PKCS12URL are provided in the `46xxsettings.txt` file, then PKCS12URL takes precedence over MYCERTURL.

The attributes of an identity certificate can be viewed by using a MIB browser in the endptMyCertTable section:

| Attribute Name | Description |
|---|---|
| endptMyCertIssuerName | Subject name of the issuer of the identity certificate |
| endptMyCertSubjectName | Subject name of the identity certificate |
| endptMyCertNotBefore | Valid from (date) |
| endptMyCertNotAfter | Valid until (date) |
| endptMyCertSN | Serial number of the identity certificate |
| endptMyCertKeyUsageExtensions | Actions available for the identity certificate |
| endptMyCertExtendedKeyUsage | Purpose of the identity certificate |
| endptMyCertAltname | Subject Alternative Name (SAN) of the identity certificate |
| endptMyCertFingerprint | SHA-1 hash of the identity certificate (Displayed by HEX string) |
| endptMyCertBasicConstraints | Basic constraints of the identity certificate |

### Server certificate validation

A server always provides a server certificate when the phone initiates a SIP-TLS, EAP-TLS or HTTPS connection.

To validate the identity of a received server certificate, the phone verifies the following:

- The certificate chain up to the trusted certificate authority in TRUSRCERTS
- The Signature
- The Revocation status through OCSP if OCSP_ENABLED is set to 1
- Certificate validity based on the current date and not-before and not-after attributes of the certificate.
- Certificate usage restrictions.
- The Identity of the server certificate that is used to connect to the server. This is optional and depends on the value of TLSSRVRID.

The following configuration parameter can be used in this context when applicable:

| Parameter name | Default value | Description |
|---|---|---|
| TLSSRVRID | 1 | Specifies how a phone evaluates a certificate trust .<br>The options are:<br>• 0: Identity matching is not performed.<br>• 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.<br>The parameter is configured through the `46xxsettings.txt`. |

Server certificate identity validation is only performed when TLSSRVRID is set to 1. When it is enabled, the phone verifies the identity contained in the server certificate. The TLS connection fails if any aspect of identity validation fails.

All TLS connections, that is, SIP-TLS and HTTPS-TLS, verify that the identity is contained in the server certificate. The server identity that is used for verification is the address that is used to connect to the server. This might be one of the following:

- IPv4 address. For example, 192.168.1.2
- IPv6 address. For example, 2001:db8::2:1
- FQDN. For example, hostname.domain.com

This identity must match an identity found in the certificate. The matching is case insensitive. The phone first checks for the server identity in the Subject Alternative Name (SAN). If it cannot be found in the SAN, then the phone checks the certificate common name (CN). This validation is based on RFC 2818.

The phone checks for an IP address server identity match with the following in the specified order until a match is found:

1. Field of type IP address in the SAN extension
2. Full content of one field in the CN

The phone checks for a FQDN server identity match with the following in the specified order until a match is found:

1. Field of type DNSName in the SAN extension. An exact match of the full string is required. For example, host.subdomain.domain.com does not match subdomain.domain.com.
2. Full content of one field in the CN using the same rules as DNSName in SAN.

**Note:**

Identities containing a wildcard are not supported and do not match. For example, *.domain.com in the certificate will not match a connection to hostname.domain.com.

In addition, all SIP-TLS connections also verify that the SIP domain configured on the phone is present in the SIP server certificate as per RFC 5922.

Use parameter ENABLE_RFC5922 to choose whether SIP domain is verified per RFC 5922 as part of certificate hostname validation.

The phone checks for a SIP domain match with the following in the specified order until a match is found:

1. Field of type URI in the SAN extension.
2. Field of type DNSName in the SAN extension and there is no URI field in the list of SAN extensions.
3. Full content of one field in the CN and there is no URI field in the list of SAN extensions.

**Note:**

Only full matches are allowed. For example, a configured SIP domain of sipdomain.com will not match a SAN DNSName containing proxy1.sipdomain.com.

**Related links**

Configuration for secure installation on page 330

# Multiple identity certificate configuration

You can configure multiple identity certificates for different applications and services, such as LDAP or PUSH. Use the SCEP, PKCS12, and DES servers to configure the identity certificates, and specify the services for which these certificates is used.

You must define the usage for each certificate allowing these certificates to be used for selected applications or services. In case the usages are not defined, the certificate is used for all configured services by default.

To individually configure the identity certificates, use the web UI or settings file.

### Usage value for SCEP and PKCS12 certificate

You can assign multiple applications or services for which each SCEP or PKCS12 certificate is used. Define the usage value from the following list:

- **SIP**: for connections with the SIP proxy.
- **Provisioning**: for connections with the provisioning server.
- **802.1x**: for 802.1x authentication.
- **LDAP**: for LDAP server.
- **Ring Central**: for connections with the RingCentral REST server.
- **Push**: for connections with the Push server.
- **PPM**: for connections with the PPM server.
- **XSI**: for connections with the XSI server.
- **Syslog**: for secure connection with Syslog server.
- **All**: for all enabled applications and services.

You can configure three certificate profile for SCEP and PKCS12. These individual certificates are identified by unique number 1, 2, and 3. For example:

SET SCEP_USAGE "Provisioning"

SET SCEP_2_USAGE "SIP,LDAP"

SET SCEP_3_USAGE "ALL"

In the above example, you have three SCEP identity certificates installed. The first identity certificate is installed for Provisioning. The second identity certificate is configured for SIP and LDAP. The third identity certificate is configured for all enabled application except Provisioning, SIP, and LDAP.

You can set the usage value to ALL, and exclude the services using !. For example: When value is set to All, !Provisioning, the identity certificate is configured for all enabled services except Provisioning.

Similarly, you can configure three certificate profiles for PKCS12 using settings file and web UI.

Refer to Parameters for configuring multiple certificates usages on page 316 for usage configuration using settings file.

### Usage value for DES certificate

You can assign applications or services for which DES certificate is used. Define the usage value from the following list:

- **Provisioning**: for connections with the provisioning server.
- **LDAP**: for connections with the LDAP server.
- **Ring Central**: for connections with the RingCentral REST server.
- **Push**: for connections with the Push server.
- **PPM**: for connections with the PPM server.
- **XSI**: for connections with the XSI server.

- **Syslog**: for secure connection with Syslog server.
- **All**: for all enabled applications and services.

You can configure only one certificate profile for DES.

## Priority order for multiple certificate installation

When multiple certificates are configured, these certificates may be configured for similar applications or services. In this case, the certificate installation is based on priority level of certificate type and certificate profile:

- Certificate type: The certificate installation is in the following priority level:
  - PKCS12
  - SCEP
  - DES

  **Note:**

  When connecting to DES, a factory certificate is used, and all identity certificates are ignored
- Certificate profile: When multiple profiles of certificates are created, such as 1, 2, or 3. Certificate profile 1 takes the highest priority, followed by profile 2 and 3.

  For example, If two SCEP (SCEP #1 and SCEP#2) certificates are installed for similar application such as LDAP. SCEP #1 takes the highest priority over SCEP #2.

**Note:**

Depending on the usage settings, there can be some applications where there are no identity certificates available. This allows an administrator the ability to prevent any identity certificate from being used on some types of connections.

## Configuring identity certificate using SCEP

### About this task

You can configure multiple certificate profiles SCEP #1, SCEP #2, and SCEP #3, and define the application or service for which the certificate is used. Use this procedure to configure the identity certificate using SCEP.

### Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **Certificates**.
3. Configure the following fields in the **Identity certificate configuration**:
   - SCEP Configuration
   - SCEP#1
   - SCEP#2

- SCEP#3

4. Configure the following option in **SCEP Configuration** field:

   **Phone behavior on pending request**: Specifies the telephone's behavior if the SCEP server indicates that the certificate request is pending manual approval.

5. Configure the following fields in **SCEP #1**:

   - **SCEP Server**: Specifies the URL address of the SCEP server.
   - **Common name**: Specifies the common name for the subject in a SCEP certificate request.
   - **Subject**: Specifies the part of SUBJECT in a SCEP certificate request that is common for requests from a different device. For example, Organizational Unit, Organization, Location, State, and Country.
   - **CA Identifier**: Specifies the Certificate Authority Identifier.
   - **Initiate renewal on % of Validity Interval**: Specifies the percentage of Validity interval of the identity certificate after which renewal procedures will be initiated.
   - **SCEP Password**: Specifies a challenge password to use with SCEP.
   - **SCEP Encryption Algorithm**: Specifies encryption algorithm for SCEP request.
   - **SCEP Usage**: Specifies a list of sources for which this certificate should be applied. You can select one or more options from the following list:
     - **SIP**: for connections with the SIP proxy.
     - **Provisioning**: for connections with the provisioning server.
     - **802.1x**: for 802.1x authentication.
     - **LDAP**: for the LDAP server.
     - **Ring Central**: for connections with the RingCentral REST server.
     - **Push**: for connections with the Push server.
     - **PPM**: for connections with the PPM server.
     - **XSI**: for connections with the XSI server.
     - **Syslog**: for secure connection with Syslog server.
     - **All**: for all enabled applications and services.

6. Perform the same configuration for other certificate profiles **SCEP #2** and **SCEP #3**, and select the usage as required.

## Configuring identity certificate using PKSC12

### About this task

You can configure multiple certificate profiles PKCS12 #1, PKCS12 #2, and PKCS12 #3, and define the application or service for which the certificate is used. Use this procedure to configure the identity certificate using PKCS12.

### Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **Certificates**.
3. Configure the following fields in **PKCS12 #1**:
   - **PKCS12 Address**: Specifies the IPv4 or IPv6 URL address, or FQDN from where a PKCS#12 file is to be downloaded.
   - **PKCS12 Password Retry Count**: Specifies the number of attempts you can make for password entry.
   - **Available Identity Certificate**: Specifies the identity certificates used as trust points for TLS connections.
   - **Upload Identity Certificate**: Displays available trust certificates for the phone.
   - **PKCS12 Usage**: Specifies a list of sources for which this certificate should be applied. You can select one or more options from the following list:
     - **SIP**: for connections with the SIP proxy.
     - **Provisioning**: for connections with the provisioning server.
     - **802.1x**: for 802.1x authentication.
     - **LDAP**: for the LDAP server.
     - **Ring Central**: for connections with the RingCentral REST server.
     - **Push**: for connections with the Push server.
     - **PPM**: for connections with the PPM server.
     - **XSI**: for connections with the XSI server.
     - **Syslog**: for secure connection with Syslog server.
     - **All**: for all enabled applications and services.
4. Perform the same configuration for other certificate profiles **PKCS12 #2** and **PKCS12 #3**.

## Configuring identity certificate using DES

### About this task

Use this procedure to configure identity certificate using DES.

### Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **Certificates**.

3. Configure the following fields in **DES**:
   - **DES Usage**: Specifies a list of sources for which this certificate should be applied. You can select one or more options from the following list:
     - **Provisioning**: for connections with the provisioning server.
     - **LDAP**: for connections with the LDAP server.
     - **Ring Central**: for connections with the RingCentral REST server.
     - **Push**: for connections with the Push server.
     - **PPM**: for connections with the PPM server.
     - **XSI**: for connections with the XSI server.
     - **Syslog**: for secure connection with Syslog server.
     - **All**: for all enabled applications and services.

## Parameters for configuring multiple certificates usages

In case of multiple identity certificates, each certificates are identified by profile number 1, 2 and 3. To configure usage for multiple identity certificates, you can set the following parameters in `46xxsettings.txt` settings file:

| Parameter name | Type | Default Value | Description |
|---|---|---|---|
| PKCS12_USAGE | String | All | Specifies the list of services for the certificate assigned to PKCS12 profile 1.<br>Valid values:<br>• SIP<br>• Provisioning<br>• 802.1x<br>• LDAP<br>• Ring Central<br>• PUSH<br>• PPM<br>• XSI<br>• Syslog<br>• All(Default)<br>In case the usage value is set to All, the certificate is configured for all enabled services.<br>You can set the value to All, and exclude the services using !.<br>For example: When value is set to All, !Provisioning, the certificate is configured for all enabled services except Provisioning. |

*Table continues…*

| Parameter name | Type | Default Value | Description |
|---|---|---|---|
| PKCS12_2_USAGE | String | All | Specifies the list of services for the certificate assigned to the PKCS12 profile 2.<br>Valid values:<br>• SIP<br>• Provisioning<br>• 802.1x<br>• LDAP<br>• Ring Central<br>• PUSH<br>• PPM<br>• XSI<br>• Syslog<br>• All(Default)<br>In case the usage value is set to ALL, the certificate is configured for all enabled services. |
| PKCS12_3_USAGE | String | All | Specifies the list of services for the certificate assigned to the PKCS12 profile 3.<br>Valid values:<br>• SIP<br>• Provisioning<br>• 802.1x<br>• LDAP<br>• Ring Central<br>• PUSH<br>• PPM<br>• XSI<br>• Syslog<br>• All(Default)<br>In case the usage value is set to All, the certificate is configured for all enabled services. |

*Table continues…*

| Parameter name | Type | Default Value | Description |
|---|---|---|---|
| SCEP_USAGE | String | All | Specifies the list of services for the certificate assigned to SCEP profile 1.<br>Valid values:<br>• SIP<br>• Provisioning<br>• 802.1x<br>• LDAP<br>• Ring Central<br>• PUSH<br>• PPM<br>• XSI<br>• Syslog<br>• All(Default)<br>In case the usage value is set to All, the certificate is configured for all enabled services. |
| SCEP_2_USAGE | String | All | Specifies the list of services for the certificate assigned to SCEP profile 2.<br>Valid values:<br>• SIP<br>• Provisioning<br>• 802.1x<br>• LDAP<br>• Ring Central<br>• PUSH<br>• PPM<br>• XSI<br>• Syslog<br>• All(Default)<br>In case the usage value is set to All, the certificate is configured for all enabled services. |

*Table continues…*

| Parameter name | Type | Default Value | Description |
|---|---|---|---|
| SCEP_3_USAGE | String | All | Specifies the list of services for the certificate assigned to SCEP profile 3.<br>Valid values:<br>• SIP<br>• Provisioning<br>• 802.1x<br>• LDAP<br>• Ring Central<br>• PUSH<br>• PPM<br>• XSI<br>• Syslog<br>• All(Default)<br>In case the usage value is set to All, the certificate is configured for all enabled services. |

## Parameters for deleting multiple identity certificate

To delete or remove multiple identity certificates, you must delete the specific identity certificates associated with a certificate profile. There are three profiles created for identity certificates in SCEP and PKCS12 each, and one profile for DES. To remove or delete any of these certificate profile, set the following parameters in `46xxsettings.txt` settings file:

For a single identity certificate installed on phone, use the DELETE_MY_CERT parameter. Set the parameter to 1 to remove the certificate.

**Note:**

DELETE_MY_CERT parameter does not work when multiple identity certificate are configured on phone.

| Parameter name | Type | Default Value | Description |
|---|---|---|---|
| DELETE_SCEP_CERT | Numeric | 0 | Specifies whether the installed identity certificate for profile SCEP#1 will be deleted.<br>Valid values:<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed.<br>When parameter value is 1, phone removes identity certificate for SCEP#1 profile. |
| DELETE_SCEP_2_CERT | Numeric | 0 | Specifies whether the installed identity certificate for profile SCEP#2 will be deleted.<br>Valid values:<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed.<br>When parameter value is 1, phone removes identity certificate for SCEP#2 profile. |
| DELETE_SCEP_3_CERT | Numeric | 0 | Specifies whether the installed identity certificate for profile SCEP#3 will be deleted.<br>Valid values:<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed.<br>When parameter value is 1, phone removes identity certificate for SCEP#3 profile. |

*Table continues…*

| Parameter name | Type | Default Value | Description |
|---|---|---|---|
| DELETE_PKCS12_CERT | Numeric | 0 | Specifies whether the installed identity certificate for profile PKCS12#1 will be deleted.<br>Valid values:<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed.<br>When parameter value is 1, phone removes identity certificate for PKCS#1 profile. |
| DELETE_PKCS12_2_CERT | Numeric | 0 | Specifies whether the installed identity certificate for profile PKCS12#2 will be deleted.<br>Valid values:<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed.<br>When parameter value is 1, phone removes identity certificate for PKCS12#2 profile. |
| DELETE_PKCS12_3_CERT | Numeric | 0 | Specifies whether the installed identity certificate for profile PKCS12#3 will be deleted.<br>Valid values:<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed.<br>When parameter value is 1, phone removes identity certificate for PKCS12#3 profile. |

*Table continues…*

| Parameter name | Type | Default Value | Description |
|---|---|---|---|
| DELETE_DES_CERT | Numeric | 0 | Specifies whether the installed identity certificate for profile DES will be deleted.<br>Valid values:<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed. |

# Identity certificate renewal

Avaya J100 Series IP Phones support an enhanced feature to install or renew/replace[3] identity certificates before expiry. The enhanced certificate management feature introduces various improvements, such as:

- Easy deployment
  - Of identity certificates for large-scale installations.
  - For a group of devices using parameter SCEP_ENTITY_CLASS.
- Improved security
  - The phone uses mutual authentication for TLS by using an existing identity certificate during the renewal process.
  - The phone generates new keys for the new certificate. However, the phone maintains the identity by retaining the same Common Name (CN) and Distinguished Name (DN).
- Quick renewal
  - Certificate renewal using the REST-based protocol to connect to Avaya Aura® System Manager.

This enhanced feature requires you to use Avaya Aura® System Manager (SMGR) version 8.1.3 or later.

For configuration information related to SMGR, see Avaya Aura System Manager/guide.

Enable the enhanced renewal feature by setting the parameter SCEP_ENTITY_CLASS value matching a corresponding value set in SMGR. Set MYCERTURL to HTTPS URL value. Refer to the Configuration for secure installation section to configure other SCEP related parameters.

## Time for renewal

Based on the expiry time of the existing certificate and the value of the parameter MYCERTRENEW, the phone initiates the certificate renewal process. The new enhanced procedure uses the REST-based protocol. However, the phone uses the SCEP protocol if necessary.

If you use the enhanced renewal feature, the parameter SCEPPASSWORD value must not be empty or set to a variable value such as $MACADDR or $SERIALNO. If you want to renew the

[3] The renewed certificate does not re-use the existing private key. During renewal, the new certificate replaces the old certificate.

certificate using the standard SCEP protocol, then remove the parameter SCEP_ENTITY_CLASS from the `46xxsettings.txt` file.

In case the phone fails to renew an identity certificate, the phone retries every 24 hours.

### Expired certificate

If an identity certificate fails renewal before expiry, you cannot use it in any new TLS, SIPs, HTTPS, or EAP authentication where mutual authentication is required. However, the existing sessions continue until you terminate it or the phone reboots.

### Managing certificate CN and DN for renewal

When you use the enhanced certificate renewal feature, the value of Common Name (CN) and Distinguished Name (DN) must match those in the existing identity certificate. The enhanced certificate renewal fails if the values are different.

If you need to update the value of CN or DN, do one of the following:

- Disable the enhanced certificate renewal feature by removing parameter SCEP_ENTITY_CLASS from the settings file.
- Use HTTP URL instead of HTTPS URL for the parameter MYCERTURL.
- Remove the existing identity certificate by using the parameter DELETE_MY_CERT.

**Related links**

Configuration for secure installation on page 330

Error handling and troubleshooting for certificate renewal on page 377

## Trusted certificates

Trusted certificates are root certificates of the certificate authority that issued the server or client identity certificates in use. These certificates are installed on the phones through the HTTP server and are used to validate server certificates during a TLS session.

System Manager includes EJBCA, an open-source PKI Certificate Authority, that can be used to issue and manage client and server certificates.

The attributes of a trusted certificate can be viewed by using a MIB browser in the endptTrustCertTable section:

| Attribute Name | Description |
|---|---|
| endptIdentityCertIssuerName | Subject name of the issuer of the trusted certificate |
| endptIdentityCertSubjectName | Subject name of the trusted certificate |
| endptIdentityCertNotBefore | Valid from (date) |
| endptIdentityCertNotAfter | Valid until (date) |
| endptIdentityCertSN | Serial number of the trusted certificate |
| endptIdentityCertKeyUsageExtensions | Actions available for the trusted certificate |
| endptIdentityCertExtendedKeyUsage | Purpose of the trusted certificate |
| endptIdentityCertAltname | Subject Alternative Name (SAN) of the trusted certificate |

*Table continues…*

| Attribute Name | Description |
|---|---|
| endptIdentityCertFingerprint | SHA-1 hash of the trusted certificate (Displayed by HEX string) |
| endptIdentityCertBasicConstraints | Basic constraints of the trusted certificate |

# 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.

# View installed phone certificates

To get the information of installed certificates on the phone, refer the web UI and phone reports. The phone application creates individual files whenever certificate information is uploaded, removed, or updated from the settings file or web UI during boot or start-up. This provides you the information of all the installed phone certificates.

**Note:**

To support use of these files, all the files in the directory structure must be readable by the craft user.

### MIB broswer

Refer to the endptMyCertTable in MIB broswer to view the multiple installed identity certificates.

### Phone report

The certificate information is available in the phone logs and phone reports. The phone report or logs collects the information from the certinfo tool, run as a craft user with simple SSH access.

## Viewing the installed certificates using the web interface

### Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **Certificates**.
3. Click **Installed Certificates**.
4. The screen displays following types of installed certificates. The scroll box against these fields displays the available certificates.
   - **Installed Trusted Certificates**: Displays all certificates installed through the parameter TRUSTCERTS.
   - **Installed OCSP Trusted Certificates**: Displays all certificates installed through the parameter OCSP_TRUSTCERTS.
   - **Installed Identity Certificates**: Displays all certificates installed through SCEP, PKCS_URL and DES.

- **Installed Custom WebServer Certificate**: Displays custom certificate for WebServer.
- **Embedded Public Certificates**: Specifies whether the embedded public root CA certificates are used for services other than Device Enrollment Service (DES).

# 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.

## 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.<br>Value operation:<br>• 0: Key Usage checking is disabled<br>• 1: Key Usage checking is enabled |

# Certificate configuration parameters

You can set the following parameters using the `46xxsettings.txt` file:

| Parameter name | Type | Default Value | Description |
|---|---|---|---|
| TRUSTCERTS | String | 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.<br>The list can contain up to 255 characters. ## Values are separated by commas without intervening spaces. |

*Table continues…*

| Parameter name | Type | Default Value | Description |
|---|---|---|---|
| MAX_TRUSTCERTS | Numeric | 10 | Specifies the maximum number of trusted certificates files defined by this parameter that can be downloaded to the phone. MAX_TRUSTCERTS enforces the number of certificates. Valid values are from 1 to 10. |
| ENABLE_PUBLIC_CA_CERTS | Numeric | 1 | Specifies whether the out-of-the-box phone can validate server certificates against a list of well-known public Certificate Authority certificates<br>Value operation:<br>• 0: Embedded public CA certificates are only trusted when TRUSTCERTS is empty.<br>• 1: Embedded public CA certificates are always trusted. |
| TLSSRVRID | Numeric | 1 | Specifies how a phone evaluates a certificate trust.<br>Value operation:<br>• 0: Identity matching is not performed.<br>• 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. |

*Table continues…*

| Parameter name | Type | Default Value | Description |
|---|---|---|---|
| FQDN_IP_MAP | String | 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 be used as an alternative to a DNS lookup or reverse DNS lookup. |
| SERVER_CERT_RECHECK_HOURS | Numeric | 24 | Specifies the number of hours after which certificate expiration and OCSP will be used, if OCSP is enabled, to recheck the revocation and expiration status of the certificates that were used to establish a TLS connection. Valid values are from 0 to 32767.<br>Value operation:<br>• 0: Periodic checking is disabled. |
| CERT_WARNING_DAYS | Numeric | 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.<br>Value operation:<br>• 0: No certificate expiration warning will be generated. |

*Table continues…*

| Parameter name | Type | Default Value | Description |
|---|---|---|---|
| DELETE_MY_CERT | Numeric | 0 | Specifies whether the installed identity certificate, using SCEP or PKCS12 file download, will be deleted.<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed. |
| BLOCK_CERTIFICATE_WILDCARDS | Numeric | 0 | Specifies whether the endpoint will accept server identity certificates with wildcards.<br>Value operation:<br>• 0: Accept wildcards in certificate.<br>• 1: Do not accept wildcards in certificates. |
| TLS_VERSION | Numeric | 0 | Specifies the TLS version used for all TLS connections (except SLA monitor agent)<br>Value operation:<br>• 0: TLS version 1.0 and 1.2 are supported.<br>• 1: TLS version 1.2 only is supported. |
| EASG_SITE_AUTH_FACTOR | String | 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 | String | 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. |
| CERT_WARNING_DAYS_EASG | Numeric | 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. |

*Table continues…*

| Parameter name | Type | Default Value | Description |
|---|---|---|---|
| ENABLE_RFC5922 | Numeric | 1 | Specifies to enable or disable the RFC5922 certificate validation.<br>Value operation:<br>• 0: disable validation<br>• 1: enable validation |

# Configuration for secure installation

For 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. |
| TLSSRVRID | 1 | Certificates installed on the servers must have the common name that matches the device configuration. |
| AUTH | 1 | Ensures usage of HTTPS file servers for configuration and software files download. Once AUTH is set to 1 and the device downloads the trusted certificates, the device can only download files from HTTPS server with certificates that can be validated using trusted certificate repository.<br>You can change this parameter value back to 0 only by resetting the phone to defaults. |
| SSH_ALLOWED | 0 | Allows to keep SSH disabled. |

### SCEP parameters

Configure the following Simple Certificate Enrollment Protocol (SCEP) parameters.

In case you are configuring multiple SCEP certificates, use the following SCEP parameters for profile 2 and 3. Refer to Multiple identity certificate configuration on page 311 for more details on multiple certificate configuration.

The SCEP parameters are not supported in IP Office environment.

| Parameter | Type | Default value | Description |
|---|---|---|---|
| MYCERTURL, MYCERTURL_2, MYCERTURL_3 | String | Null | Specifies the URL to access 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.<br><br>To specify the SCEP URL for profile 2 and 3, use MYCERTURL_2 and MYCERTURL_3. |
| MYCERTCN, MYCERTCN_2, MYCERTCN_3 | String | $SERIALNO | Specifies the Common name (CN) for SUBJECT in SCEP certificate request.<br><br>The value must be a string that contains either $SERIALNO (which is replaced by the phone serial number in upper case) or $MACADDR (which is replaced by the phone MAC address in lower case), but it can contain other characters as well, including spaces.<br><br>$MACADDR_UPPER is replaced by the same value as $MACADDR but in upper case.<br><br>In order to use enhanced certificate renewal in SMGR 8.1.3 and later, the value of MYCERTCN parameter must remain unchanged from the one used in existing identity certificate. Enhanced certificate renewal fails if this value is changed. If a new value is explicitly desired, then either remove the parameter SCEP_ENTITY_CLASS or remove the existing certificate by using DELETE_MY_CERT parameter and re-install a new one.<br><br>To specify the CN name for SCEP certificate profile 2 and 3, use MYCERTCN_2 and MYCERTCN_3. |
| MYCERTDN, MYCERTDN_2, MYCERTDN_3 | String | Null | Specifies 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.<br><br>In order to use enhanced certificate renewal in SMGR 8.1.3 and later, the value of MYCERTDN parameter must remain unchanged from the one used in existing identity certificate. Enhanced certificate renewal fails if this value is changed. If a new value is explicitly desired, then either remove the parameter SCEP_ENTITY_CLASS or remove the existing certificate by using DELETE_MY_CERT parameter and re-install a new one.<br><br>For certificate profile 2 and 3, use MYCERTDN_2 and MYCERTDN_3. |

*Table continues…*

| Parameter | Type | Default value | Description |
|---|---|---|---|
| MYCERTKEYLEN, MYCERTKEYLEN_2, MYCERTKEYLEN_3 | 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.<br>For certificate profile 2 and 3, use MYCERTKEYLEN_2 and MYCERTKEYLEN_3. |
| MYCERTRENEW, MYCERTRENEW_2, MYCERTRENEW_3 | Numeric | 90 | Specifies the percentage of the identity certificate's validity interval after which renewal procedure will be initiated. The value is 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 REST based protocol or SCEP server again to renew the certificate. The range is from 1 to 99.<br>For example: if you set the MYCERTRENEW 90, certificate validity is 365 days, the renewal time is calculated as = (365)-(365*90%)= 36.5 days before the expiry.<br>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.<br>For certificate profile 2 and 3, use MYCERTRENEW_2 and MYCERTRENEW_3. |
| MYCERTCAID, MYCERTCAID_2, MYCERTCAID_3 | String | CAIdentifier | Specifies the Certificate Authority Identifier. Certificate Authority servers may require a specific CA Identifier string in order to accept GetCA requests. If the device works with such a Certificate Authority, the CA identifier string can be set through this parameter.<br>For certificate profile 2 and 3, use MYCERTCAID_2 and MYCERTCAID_3. |

*Table continues…*

| Parameter | Type | Default value | Description |
|---|---|---|---|
| SCEPPASSWORD, SCEPPASSWORD_2, SCEPPASSWORD_3 | 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.<br>If the value contains $SERIALNO, $SERIALNO is replaced by the phone serial number in upper case. If the value contains $MACADDR, $MACADDR is replaced by the phone MAC address in lower case without the colon separators. $MACADDR_UPPER is replaced by the value in upper case.<br>In order to use enhanced certificate renewal in SMGR 8.1.3 and later, SCEPPASSWORD value cannot be empty nor it can be set to a variable such as $MACADDR or $SERIALNO.<br>If renewal or enrollment of a certificate is performed using standard SCEP protocol, then parameter SCEP_ENTITY_CLASS must be removed.<br>For certificate profile 2 and 3, use SCEPPASSWORD_2 and SCEPPASSWORD_3. |
| SCEPENCALG, SCEPENCALG_2, SCEPENCALG_3 | Numeric | 0 | Specifies SCEP Encryption Algorithm.<br>Value operation:<br>• 0: DES<br>• 1: AES-256<br>For certificate profile 2 and 3, use SCEPENCALG_2 and SCEPENCALG_3.<br>**Note:**<br>Avaya J129 IP Phone supports this parameter. |
| SCEP_ENTITY_CLASS, SCEP_ENTITY_CLASS_2, SCEP_ENTITY_CLASS_3 | String | Null | Specifies to use the enhanced SCEP enrollment request. The value of entity-class is set in SMGR.<br>For certificate profile 2 and 3, use SCEP_ENTITY_CLASS_2 and SCEP_ENTITY_CLASS_3. |

# 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 334

# 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.<br>Setting the value to 1 specifies only FIPS-approved cryptographic algorithms are supported.<br>Value operation:<br>• 0: No restriction on using non-FIPS approved cryptographic algorithms.<br>• 1: Use only FIPS-approved cryptographic algorithms using embedded FIPS 140-2-validated cryptographic module. |

**Related links**

FIPS mode on page 333

# Chapter 10: 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 337

# 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 337

# 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 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.<br>When this parameter is enabled, the phone doesn't store any personal data without encryption for a period of more than 24 hours.<br>Value operation:<br>• 0: Secure mode is disabled (default)<br>• 1: Secure mode is enabled |

# 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 344

# 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.<br>Value operation:<br>• 0: Non-secure mode using UDP transport<br>• 1: Secure mode using TLS transport RFC 5425<br>Selected value is available as Default option in Administrator menu |

**Related links**

Secure Syslog on page 344

# 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 11: Failover and survivability

## Redundancy with IP phone and Avaya Aura®

Avaya IP phones and Avaya Aura® Communication Manager can be configured to provide optimal redundancy support. The phones can be configured to register simultaneously with the following:

- Two Avaya Aura® Session Manager SIP proxies
- Two Session Manager instances and one Branch Session Manager
- One Session Manager and one Branch Session Manager

If the connection is lost to the primary Session Manager, the phone establishes communications with the second Session Manager. Similarly, if the second Session Manager is unavailable, then the phone establishes communication with the third Session Manager. The third Session Manager can only be a Branch Session Manager.

Alternatively, a non-Avaya Aura proxy can be used as a survivable proxy. In this case, when the connection is lost between the phone and the Session Manager, the phone again registers with the non-Avaya Aura proxy and attempts to continue the service with little disruption. The two possible non-Avaya Aura configurations are as follows:

- One Session Manager and one non-Avaya Aura proxy
- Two Session Manager instances and one non-Avaya Aura proxy

If connection between a phone and Session Manager is lost during a call, then the phone attempts to preserve the call by sustaining the audio path between the two parties. This is called call preservation. In spite of this best effort service, the audio path might be lost. Further, in a preserved call, the phone does not support call features, for example, conference call, call transfer, and call forward.

## Detection of loss of connection

The three methods to detect a loss of connection between the phone and the SIP proxy are as follows:

- Loss of TCP connection between the phone and the SIP proxy: If the TCP socket closes, or if the TCP keep alive timer times out, then there is a loss of connection. The TCP keep alive timer is set to a default value of 45 seconds but can be modified by using the TCP_KEEP_ALIVE_TIME parameter in the `46xxsettings.txt` file.

- Failure of the proxy to respond to a SIP INVITE message within a specified time: If the phone sends a SIP INVITE message to the proxy and the proxy does not reply within a specified time, then there is a loss of connection. The response time is set to a default value of 5 seconds in the `46xxsettings.txt` file but can be modified by using the FAST_RESPONSE_TIMEOUT parameter. The Avaya Aura® System Manager parameter, TIMER B, takes precedence over the `46xxsettings.txt` file parameter.
- Failure of the proxy to respond to a SIP registration method: After the initial registration, the phone sends a re-registration message periodically to the proxy. If the proxy fails to respond to the re-registration message, the phone starts a failover. The parameter REGISTERWAIT in the `46xxsettings.txt` file defines the period of re-registration. However, the Avaya Aura® System Manager parameter Registration Expiration Time takes precedence over the `46xxsettings.txt` file parameter.

# Failover to a backup proxy

When a loss of connection occurs, the phone continues the service with the secondary Session Manager. If the secondary Session Manager is unavailable, the phone uses the survivable proxy.

# Restoring the phone to the primary proxy

When the link between the phone and the primary Session Manager is restored, the phone might re-establish communication and revert to the primary Session Manager. This process is referred to as failback.

After a failover occurs, the phone waits for a period of time defined by the RECOVERYREGISTERWAIT parameter and then the phone attempts to register back to the primary proxy. You can modify the time in the Reactive Monitoring parameter on System Manager. This parameter takes precedence over the `46xxsettings.txt` file parameter. After this timer expires, the phone attempts to connect to the primary Session Manager. If the attempt is successful, the phone sends a new SIP registration message to the Primary Session Manager. At this point, another timer starts that is defined by the parameter WAIT_FOR_REGISTRATION_TIMER. If there is no response to the registration message from the proxy by the time it expires, then it waits for the RECOVERYREGISTERWAIT time.

This process maps to the `46xxsettings.txt` file parameter FAILBACK_POLICY being set to automatic. If the parameter is set to manual, then the administrator must send a message to the phone through System Manager to force it to re-register with the primary Session Manager.

# Proxy determination when the phone loses connection to the primary proxy

During the initial configuration, you must provide a list of available SIP proxies to which the phone can connect. You must prioritize the proxies into primary, secondary, and survivable proxies.

Initially, to provide the list of prioritized proxies, you can use DHCP, LLDP, or the `46xxsettings.txt` file. After the phone connects to Avaya Aura® Session Manager, Avaya Aura® System Manager provides a new list of proxies. This list precedes over other configuration sources. In System Manager, use the following fields to list the proxies:

- **Primary Session Manager**
- **Secondary Session Manager**
- **Survivability server**

If the phone detects a loss of connection with the primary proxy, the phone fails over to the secondary proxy. If the primary and secondary proxies are unreachable, the phone fails over to the survivable proxy.

# Simultaneous registration

The phones can simultaneously register with multiple proxies. Simultaneous registration enables quick and deterministic redundancy. When configuring the phones for redundancy with Avaya Aura®, set the SIPREGPROXYPOLICY parameter to `Simultaneous`. When the phone registers to a SIP proxy for the first time, the SIPREGPROXYPOLICY parameter forces simultaneous registration to multiple proxies. Use the SIMULTANEOUS_REGISTRATIONS parameter to specify the number of simultaneous proxies.

The phone supports up to five proxies for simultaneous registration.

**Note:**

All Session Manager and Branch Session Manager instances support simultaneous registration. Non-Avaya Aura® proxies do not support simultaneous registration. For example, if your configuration is two Session Manager instances and a non-Avaya Aura® proxy, set the value of SIMULTANEOUS_REGISTRATIONS to `2`.

# Limitations during failover or failback

Limitations of the phone when the phone is in the process of failover or failback are as follows:

- Held calls are dropped.

- Calls that are in the middle of the conferencing or transfer set up are dropped.
- Calls in the dialing or ringing state might not be completed.
- Emergency calls might not work depending on the stage of failover and the functionality available on the alternate server.
- Incoming calls might not be completed, or they might get diverted to voicemail.
- Message Waiting Indicator is cleared.

# Preserved call

When there is a call in progress and a loss of connection occurs between the phone and the proxy, an attempt is made to preserve the audio path between the phone and the far end. This is called Call preservation. In most cases, call preservation is successful. However, there are conditions when the audio path is lost. This loss of audio might happen when there is no direct path between the phone and the far end. The entity that connects the media between the two ends is also affected by the loss. Further, there are limitations to modify a preserved call.

## Limitations of call preservation

A call is preserved on a best effort basis. If the audio path is directly between two devices and there is no network issue between the two devices, the audio path is preserved. If the audio is anchored by a device in the middle, for example, a gateway or conference server and that device is affected by the network outage, there will not be any audio path. In a preserved call, the phone does not support call features, for example, conference call, call transfer, and call forward . The reason is loss of signaling between the phone and the SIP proxy that was used when the call was initially established.

The loss of signalling between the phone and the originating proxy also limits the call control between the preserved calling parties. For example,

- Calls cannot be transferred.
- Call conferencing cannot be initiated.

If a user disconnects a preserved call, the other end might not be disconnected because of the loss of signaling.

# Limitations after a successful failover

### Failover to a Session Manager

After a phone successfully fails over to a secondary Session Manager, all features and functionality work properly for new calls. However, there are limitations to modify a preserved call.

### Failover to a Branch Session Manager

After a phone successfully fails over to Branch Session Manager, the value of the parameter FAILBACK_POLICY changes to Admin. In this case, you must go to the System Manager and manually re-register the phone with Session Manager.

**Note:**

Administration of Session Manager and Branch Session Manager nodes are explicitly required in the System Manager user record.

### Failover to a proxy other than Avaya Aura®

The limitations after a phone fails over to a proxy other than Avaya Aura® are:

- A conference is limited to three parties and is hosted by the phone.
- Contacts can be used and new contacts can be saved on the phone. New contacts are cached on the phone, and after failback to Avaya Aura®, the new contacts are synchronized with Avaya Aura®.
- The dial plan for Avaya Aura® is unavailable. Instead, the dial plan configured in the `46xxsettings.txt` file is used.
- The following Avaya Aura® features are unavailable:
  - Last party drop
  - Send All Calls (Do Not Disturb)
  - Presence
  - Calling party block/unblock
  - Call park/unpark
  - All forms of call pickup
  - Priority calls
  - MLPP functionality
  - Auto callback
  - Malicious call trace
  - EC500 on/off
  - Transfer to voicemail
  - Paging
  - Call recording
  - Bridge Line Appearance
  - Extend call
  - Hold recall
  - Transfer recall
  - Busy Indicator
  - Message Waiting Indicator

- Team button
- Call Center Elite

# Indications of redundancy

The following indications are given to the user when the phone has connection issues:

### Acquiring service

When a phone does not have a communication channel established with any SIP proxy and a call is in progress; the phone displays the `Limited Phone Service` message. The message disappears automatically, or the user can cancel it. An icon indicating Acquiring Service is displayed on the top line of the phone. This icon does not go away until a communication channel is established with a SIP proxy. The icon is an exclamation mark within a triangle similar to the following:

If there is no ongoing call and there is no communication channel between the phone and the proxy, then the phone displays the message `Acquiring Service`.

**Note:**

If you set PROVIDE_LOGOUT to 0, the phone does not display the **Cancel** soft key for the user. The phone logins automatically after a communication channel is established with a SIP proxy.

### Preserved call

When a failover occurs, and a call is preserved, the call appearance line of the phone displays the following preserved call Indicator:



# Supported non Avaya Aura® proxies for redundancy

The supported non Avaya Aura® proxies for redundancy are as follows:

- Avaya Secure Router 2330 and 4134
- Avaya IP Office
- Audiocodes MediaPack™ 11x series and Mediant™ series gateways

**Note:**

All secondary gateways must be configured to support connection reuse.

# Parameters for redundancy provisioning

## SIP connection parameters

| Parameter name | Default value | Description | System Manager parameter name |
|---|---|---|---|
| CONTROLLER_SEARCH_INTERVAL | 16 | Specifies the number of seconds the phone will wait to complete the maintenance check for monitored controllers.<br>Valid values are from 4 to 3600. | NA |
| DISCOVER_AVAYA_ENVIRONMENT | 1 | Specifies dynamic feature set discovery<br>Value operation:<br>• 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.<br>• 0: The phone operates in a mode where AST features are not available.<br>**Note:**<br>Set the parameter to 0 for IP Office environment. | NA |

*Table continues…*

| Parameter name | Default value | Description | System Manager parameter name |
|---|---|---|---|
| FAST_RESPONSE_TIMEOUT | 4 | Specifies the number of seconds the phone will wait before terminating an invite transaction if no response is received.<br>Valid values are from 0 to 32.<br>Value operation:<br>• 0: Timer is disabled | Timer B<br>This parameter is mandatory in System Manager and the default value is 2 seconds. The value set in System Manager overwrites the value in the `46xxsettings.txt` file. |
| RECOVERYREGISTERWAIT | 60 | Specifies the number of seconds. If no response is received by WAIT_FOR_REGISTRATION_TIMER to a REGISTER request within the specified number of seconds, the phone tries again after a randomly selected delay of 50% to 90% of the value of RECOVERYREGISTERWAIT.<br>Valid values are from 10 to 36000. | Reactive Monitoring |
| REGISTERWAIT | 900 | Specifies the number of seconds for next re-registration to the SIP proxy.<br>Valid values are from 30 to 86400 seconds. | Registration Expiry Timer<br>The value set in System Manager overwrites the value in the `46xxsettings.txt` file. |
| WAIT_FOR_REGISTRATION_TIMER | 32 | Specifies the number of seconds the phone will wait for a response to a REGISTER request. If no response message is received within this time, the phone tries to register again based on the value of RECOVERYREGISTERWAIT.<br>Valid values are from 4 to 3600. | NA |

*Table continues…*

| Parameter name | Default value | Description | System Manager parameter name |
|---|---|---|---|
| SIP_CONTROLLER_LIST | Null | Specifies a list of SIP controller designators, separated by commas without any intervening spaces. When this parameter has multiple IP addresses, the list order defines the priority of the controllers for selection during a failover. The first element of the list has the highest priority, and the last element has the lowest priority. | Primary Session Manager, Secondary Session Manager and Survivability server |
| ENABLE_PPM_SOURCED_SIPPROXYSRVR | 1 | Enables PPM as a source of SIP proxy server information.<br>Value operation:<br>• 0: Proxy server information received from PPM is not used.<br>• 1: Proxy server information received from PPM is used. | NA |
| SIP_CONTROLLER_LIST_2 | Null | Replaces SIP_CONTROLLER_LIST for IPv4 and IPv6 phones. It is used to select the registration address. | Primary Session Manager, Secondary Session Manager, and Survivability server. |
| SIMULTANEOUS_REGISTRATIONS | 5 | Specifies the number of simultaneous Session Manager and Branch Session Manager registrations that the phone must maintain.<br>Valid values are from 1 to 5.<br>The value of this parameter must not be less than the number of core Session Manager instances in SIP_CONTROLLER_LIST. | NA |

*Table continues…*

| Parameter name | Default value | Description | System Manager parameter name |
|---|---|---|---|
| SIPREGPROXYPOLICY | Simultaneous | Specifies whether the telephone will attempt to maintain one or multiple simultaneous registrations.<br>Value operation:<br>• Alternate: The phone registers only to the first controller in the list. If the phone cannot reach the first controller, the phone registers to the second controller. This value is supported only in IP Office environment.<br>• Simultaneous: The phone simultaneously registers to more than one SIP proxy controller at the same time. This value is supported only in Avaya Aura® environment. | NA |

The primary, secondary, and survivable server settings for a phone must be configured in System Manager. This enables the phone to access the full list of assigned servers after the phone logs in. You must provide at least one primary and secondary server to the phone to make the initial login connection. You can provide the servers by using DHCP, LLDP, or the `46xxsettings.txt` file parameters SIP_CONTROLLER_LIST or SIP_CONTROLLER_LIST_2. Ideally, the full list of servers must be provided. However, when a survivable server is location specific, you must only include the survivable server in DHCP, LLDP or the `46xxsettings.txt` file if the correct survivable server for the location can be provided. This ensures that the phone always receives the correct survivable server address. A DHCP server local to a branch is one such method in which this could be done. However, if you cannot provide the correct location-specific survivable server reliably in DHCP, LLDP, or the `46xxsettings.txt` file, then you must not include it. In this case, the phone gains access to it after login.

### Dial Plan parameters for use when failing over to a proxy other than Avaya Aura

| Parameter name | Default value | Description |
|---|---|---|
| ENABLE_REMOVE_PSTN_ACCESS_PREFIX | 0 | Enables the removal of the PSTN access prefix from the collected dial strings when the phone communicates with a non-AST controller.<br>Value operation:<br>• 0: PSTN access prefix digit is not removed.<br>• 1: PSTN access prefix digit is removed from the collected digit string before formulating the INVITE for delivery to the controller.<br>The parameter has no effect if you enable this parameter when the phone communicates with an AST-capable controller. |
| PSTN_VM_NUM | Null | Specifies a phone number or Feature Access Code to be used by the messaging application in a non-Avaya or failover server environment. This dialable string is used to call into the messaging system, for example, when you press the Message Waiting button. |
| INTER_DIGIT_TIMEOUT | 5 | Specifies the timeout that takes place when a user stops entering digits. The timeout is treated as digit collection completion, and when it occurs, the application sends out an invite.<br>Valid values are from 1 to 10. |
| ENABLE_REMOVE_PSTN_ACCESS_PREFIX | | Enables the phone to perform digit manipulation during failure scenarios. This parameter enables removal of the PSTN access prefix from the outgoing number.<br>Value operation:<br>• 0: PSTN access prefix is retained in the outgoing number<br>• 1: PSTN access prefix is stripped from the outgoing number. |
| PHNLAC | | Indicates the local area code of the phone. . PHNLAC is a string that enables users to dial local numbers with more flexibility when used together with the LOCAL_DIAL_AREA_CODE parameter. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| 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. |
| LOCAL_DIAL_AREA_CODE | | Specifies whether a user must dial the area code for calls within the same area code regions.<br>Value operation:<br>• 0: Users do not need to dial an area code.<br>• 1: Users need to dial an area code. |
| DIALPLAN | Null | Specifies the dial plan used in the phone. It accelerates dialing by eliminating the need to wait for the INTER_DIGIT_TIMEOUT timer to expire. |

# Redundancy in a non-Avaya proxy environment

In an Avaya environment, the SIP proxy list is defined using dotted decimal notation to define the proxy addresses. In a non-Avaya environment, where FQDNs are used to define the SIP proxy, there can only be one proxy. In this case, redundancy is only supported in Broadsoft environment.

# Chapter 12: Backup and restore

## User profile backup on Personal Profile Manager (PPM)

The Personal Profile Manager (PPM) provides a web services interface for endpoints to connect to the network to download profile data and store data back in the network for easy access across multiple user devices.

The phone saves all the user settings on the PPM in an Avaya Aura® environment. When the user logs in to any registered device, PPM restores all user data on the device. For more information about backup and restore, see *Administering Avaya Aura® System Manager*.

**Related links**

Personal Profile Manager on page 86

## User profile parameters for backup

The table lists a few parameters backed up on Personal Profile Manager (PPM). These are internal parameters corresponding to the user settings on the phone and are not available on the `46xxsettings.txt` file. For more information about backup and restore, see *Administering Avaya Aura® System Manager*.

| Parameter | Default value | Description |
|---|---|---|
| CLICKS | 1 | Specifies whether the phone button click sound is ON. |
| CALL_PICKUP_RING_TYPE | 1 | Specifies the default ring type for call pickup. |
| OUTSIDE_CALL_RING_TYPE | 1 | Specifies the default call ring type for an external call. |
| CALL_PICKUP_INDICATION | 3 | Specifies the call pickup indication. The following are the types of call pickup indication:<br>• Audio<br>• Visual<br>• None |
| TIMEFORMAT | 0 | Specifies whether the time format is the AM-PM format or the 24–hour format. |
| DATE_FORMAT_OPTIONS | 1 | Specifies the date display format. |
| CALL_LOG_ACTIVE | 1 | Specifies whether the call log is active. |

*Table continues…*

| Parameter | Default value | Description |
|---|---|---|
| DEFAULT_CONTACTS_STORE | 1 | Specifies the default account where all user contacts are stored. |
| ENABLE_PHONE_LOCK | 0 | Specifies whether Lock soft key and a feature button are displayed on the phone. |
| SHOW_CALL_APPEARANCE_NUMBERS | 0 | Specifies whether the phone displays call appearance numbers in the call containers. |

# Chapter 13: Maintenance

## 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 logging in on page 92

# 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 **Syslog enabled** and press **Toggle** to select.
9. **(Optional)** Scroll to **Syslog server** and enter the IP address or FQDN.
10. **(Optional)** Scroll to **Log server secure** and press **Toggle** to select a secure or non-secure mode to send syslog.
11. Press **Save**.

**Related links**

Accessing the Admin menu after logging in on page 92

# 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 | |
| **Syslog enabled** | Specifies the enabling or disabling syslog messages.<br>The options are:<br>• **Off (default)**<br>• **On** |

*Table continues…*

| Name | Description |
|---|---|
| **Syslog Server** | Specifies the IP or the DNS address of the Syslog server. For secure syslog mode, you must use an FQDN address.<br>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.<br>The options are:<br>• **Off (default)**<br>• **On** |
| **Log Level** | Specifies the severity level of the syslog messages. Events with the selected severity level and above are logged.<br>The options are:<br>• **Emergencies**<br>• **Alerts**<br>• **Critical**<br>• **Errors (default)**<br>• **Warnings**<br>• **Notices**<br>• **Information**<br>• **Debug** |
| **Log Categories** | Specifies the list of log categories.<br>Select the appropriate log category. For example, select category **Audio** for generating audio logs.<br>The default value is empty. |
| **Enhanced Debugging** | Specifies the status of enhanced debugging.<br>The options are:<br>• **Enable**<br>• **Disable (default)** |
| SNMP | |
| **SNMP String** | Specifies the SNMP community name string.<br>The valid value is a string of up to 32 ASCII alphanumeric characters. The default value is empty. |

*Table continues…*

| Name | Description |
|---|---|
| **SNMP Address** | Specifies the IP addresses for SNMP queries.<br>The valid value is a string of up to 255 ASCII characters without any intervening spaces.<br>The default value is empty. |
| Packet Capture | |
| **Packet Capture** | Captures the phone network traffic.<br>See Capturing the phone network traffic on page 184 |
| Phone Report | |
| **Phone Report Server Address** | Specifies the file server address to send the phone report. Click **Generate Phone Report**.<br>The valid value is a string of up to 255 ASCII characters.<br>**Note:**<br>The phone report also provides details such as product ID, default server type, and Device Enrollment Service (DES) support information. |
| SSH | |
| **SSH Allowed** | Specifies whether Secure Shell (SSH) is supported.<br>The options are:<br>• **Enable**<br>• **Disable (default)**<br>• **Configured using local administrative procedure** |
| **SSH Idle Timeout** | Specifies the time in minutes after which SSH is disabled.<br>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.<br>The valid value is a string of up to 255 ASCII characters. The default value is empty. |
| **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.<br>The valid value is a string of up to 64 ASCII characters. The default value is empty.<br>**Note:**<br>You can add a maximum of four certificates. |

*Table continues…*

| Name | Description |
|---|---|
| **EASG site Authentication Factor code** | Specifies the Site Authentication Factor code associated with the EASG site certificate installed.<br>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 the phone screen displays a warning message for the first.<br>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.<br>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.<br>The options are:<br>• **Disable (default)**<br>• **Enable with payloads removed from RTP packets**<br>• **Enable with payloads included in RTP packets**<br>• **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.<br>The options are:<br>• **Disable (default)**<br>• **Enable**<br>• **Controlled from Admin Menu** |
| **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.<br>The options are:<br>• **Enable**<br>• **Disable (default)** |

*Table continues…*

| Name | Description |
|---|---|
| **UDP Port for discovery and test messages** | Specifies the port used to receive packets from an SLA Monitor server.<br>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.<br>The valid values are:<br>• **Production (Default)**: the dynamic evaluation of the acoustic protection is active.<br>• **Debugging**: the dynamic evaluation of the acoustic protection is inactive. |
| **Acoustic exposure config mode** | Specifies the acoustic exposure dynamic range.<br>The valid values are:<br>• **Acoustic protection off (Default)**<br>• **Acoustic protection On (Default)** |
| **Sliding Window Size** | Specifies the window size for acoustic protection.<br>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.<br>The options are:<br>• **Adjunct**<br>• **Disable**<br>The default value is Adjunct. |

# Capturing the phone network traffic

## About this task

Use the phone network traffic data to debug phone registration and call-related issues. Use the phone web interface to capture the real-time network traffic of the phone. The phone sends the network traffic data to the computer from which 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 network traffic while you run the report.

Use IPv4 network for Avaya J129 IP Phone.

### 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 according to 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.

# 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 342 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 110 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

Avaya J100 Series IP Phones are upgraded to a newer version using the APPNAME parameter. Alternatively, you can use the APPNAME_IN _USE parameter which checks the firmware version installed on the phone to perform a corresponding upgrade action, for example:

```
IF $APPNAME_IN_USE SEQ 4.0.2.0.11 GOTO CROSSGRADE
```

The device process using the APPNAME parameter is described below:

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 currently installed software version with the version specified in the APPNAME parameter.
5. If the firmware version specified in the APPNAME parameter differs from the currently running software version, the phone downloads the software files for upgrade.
6. The phone automatically restarts to apply the upgraded firmware.

**Tip:**

The upgrade events are logged under NOTICES level in the `Syslog` file.

# Server-initiated update

With the Server-initiated update feature, you can get a notification from the SIP server when there is a new software or file available on the file server. The Server-initiated update feature is disabled by default. To enable this feature, you must set the ENABLE_OOD_RESET_NOTIFY parameter to 1.

When the phone receives a SIP NOTIFY message about available updates, the phone compares the firmware version in the `J100Supgrade.txt` file on the file server with the current version installed. If the file server has the latest firmware, the phone reboots and upgrades.

If there is an updated settings file on the server, the phone downloads the files to apply the new settings. Depending on the parameters that change, the phone logs out the current user or reboots. If there are active calls or other transmissions, the phones apply the new settings when the status is idle.

The Status tab in the web interface displays the date and time of the last update.

You can use either of the following to get the notification from the SIP server:

- the Administration menu on the phone

- the Management tab in the web interface

**Related links**

Updating phone settings and firmware on page 113
Management settings field descriptions on page 176
Status field description on page 121

# 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 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 369
Management settings field descriptions on page 176

# 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.<br>The options are:<br>• 0: Disabled<br>• 1: Daily<br>• 2: Weekly<br>• 3: Monthly<br>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.<br>Mon, Tue, Wed, Thu, Fri, Sat, Sun for a weekly update.<br>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.<br>The phone uses the default value if you set invalid values.<br>Example for weekly update: SET AUTOMATIC_UPDATE_DAYS "Sun"<br>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.<br><br>Each phone picks a random time between this specified window.<br><br>The time is in 24hr format.<br><br>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.<br><br>For "22,2". Sets 4 hour window from 10 p.m. to 2 a.m. next day for the automatic update.<br><br>For "0,0". Sets 24 hour window from 00 a.m. to 00 a.m. next day for the automatic update.<br><br>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.<br><br>AUTOMATIC_UPGRADE_INSTALL_DATE_TIME is applicable if AUTOMATIC_UPDATE_POLICY is set to 1, 2, or 3.<br><br>The format is YYYY-MM-DDThh:mm, where:<br>• YYYY is a 4 digit numeric value for the year, MM is a 2 digit numeric value for the month<br>• DD is a 2 digit numeric value for the date, which is 1 to 31<br>• T is the time separator<br>• hh is a 2 digit numeric value for hours of the day which is 00 to 23<br>• mm is a 2 digit numeric value for minutes of the hour, which is 00 to 59<br><br>For example, SET AUTOMATIC_UPGRADE_INSTALL_DATE_TIME 2015-04-12T23:20<br><br>Note that this parameter applies to the local time of the phone as defined by the following parameters:<br>• GMTOFFSET<br>• DAYLIGHT_SAVING_SETTING_MODE<br>• DSTOFFSET<br>• DSTSTART<br>• 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.<br><br>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.<br><br>The options are:<br><br>• 0: The phone does not display the reboot confirmation prompt. Instead it updates the phone directly.<br><br>• 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 369
Management settings field descriptions on page 176

# 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? | N/A | |

*Table continues…*

| No. | Task | Reference | ✔ |
|---|---|---|---|
| 2 | Are you able to make a call from the phone? | For more information, see device specific using guide. | |
| 3 | Are you able to modify the phone settings file parameters and end user settings. | List of configuration parameters on page 383 | |
| 4 | Are you able to upgrade your phone? | Device upgrade process on page 368 | |
| 5 | For security considerations, have you configured the phone setup with TLS signaling? Have you installed the appropriate private network authentication certificates? | Certificate management on page 308 | |
| 6 | It is critical that you verify Emergency calling is working properly in your network. It may be necessary to make arrangements with the appropriate authorities to test this functionality. | For more information, see *Administering emergency numbers* | |

**Note:**

For more information about IP Office specific installation, see the following IP Office documents:

- Avaya IP Office™ Platform Solution Description
- Avaya IP Office™ Platform Feature Description

# Chapter 14: Troubleshooting

## Phone displays Acquiring Service screen

### Cause

The configured SIP proxy servers are not accessible from the phone.

***Solution***

1. On the Acquiring Service screen, press **Cancel** to logout from the phone and go to the **Admin** menu.
2. Press **SIP** > **SIP proxy server**.
3. Check the number of SIP proxy servers that are configured. If the connections are properly configured, then ensure the following:
   - SIP proxy servers are specified by IP address and not by FQDN.
   - There are only two proxy servers configured.

   A filled in circle implies a successful configuration. A circle with a line through it implies a failed connection.

### Cause

The configured SIP proxy servers are accessible. However, TLS is being used and there is an issue with the certificate configuration.

***Solution***

1. On the Acquiring Service screen, press **Cancel** to logout from the phone and go to the **Admin** menu.
2. Press **SIP** > **SIP global settings**.
3. Use the **Up** and **Down** arrow keys to go to the Reg. policy screen.
4. Use the **Left** arrow key to configure the Reg. policy as **Alternate** and press **Save**.
5. Use the **Up** and **Down** arrow keys to go to the Avaya Environment screen.
6. Use the **Left** arrow key to configure the Avaya Environment as **No** and press **Save**.

### Cause

There is a problem with the SIP proxy configuration.

***Solution***

1. On the Acquiring Service screen, press **Cancel** to logout from the phone and go to the **Admin** menu.
2. Press **SIP** > **SIP proxy server**.
3. If one or more configured SIP proxy server connections shows as failed, press **Ping**.

   The circle is filled in if the connection is properly configured. Circle with a line through it is a failed connection.
4. Ping each SIP proxy server.

# SLA Mon™ agent

SLA Mon™ technology is a patented Avaya technology embedded in Avaya products to facilitate advanced diagnostics. The phones support SLA Mon™ agent, which works with Avaya Diagnostic Server (ADS). By setting the parameter SLMSTAT to 2, you can enable the feature for remote worker deployments or cloud environments.

SLA Mon™ server controls the SLA Mon™ agents to execute advanced diagnostic functions, such as:

- Endpoint diagnostics
  - Remotely control IP phones to assist end-users with IP phone configuration and troubleshooting.
  - Remotely generate single and bulk test calls between IP phones.
  - Remotely execute limited packet captures on IP phones to troubleshoot and diagnose IP phone network traffic.
- Network monitoring
  - Monitor multiple network segments for performance in terms of packet loss, jitter, and delay.
  - Monitor hop-by-hop QoS markings for voice and video traffic.

**Note:**

Add the root-trusted certificate of the SLA Mon™ server certificate to the trusted certificate list administered using TRUSTCERTS.

For example: SET TRUSTCERTS `slamonRootCA.crt, rootCertRNAAD.cer`

# Error handling and troubleshooting for certificate renewal

If the certificate renewal or enrollment fails, the phone screen displays one of the following messages:

- `SCEP certificate installation failed`
- `REST certificate renewal failed`

You can obtain error details in the corresponding debug logs of the phone with the CERTMGMT category. The following are the examples of common errors and solutions to fix:

| Error | Possible cause and solution |
|---|---|
| Incorrect password | Ensure the passwords in the `46xxsettings.txt` file and SMGR are the same. |
| 401 unauthorized response received | The Common Name (CN) or Distinguished Name (DN) of the current renewal request does not match the existing certificate. Refer to section Managing certificate CN and DN for renewal. |
| 403 response received during initial SCEP or certificate re-issuance | Entity Class in SMGR has expired. Extend the validity of entity class in SMGR. |
| 404 response received during certificate re-issuance | SMGR is not upgraded to 8.1.3 successfully. |
| TLS handshake error | The phone trust CA list does not contain the SMGR root cert. |

For further troubleshooting, you can refer to Avaya Aura® System Manager logs through CLI access and view the following files:

- `/var/log/Avaya/jboss/log/ejbca.log`
- `/var/log/Avaya/jboss/log/server.log`
- `/var/log/Avaya/mgmt/tm/tmAuditLog.log`
- `/var/log/Avaya/mgmt/tm/tmTraceLog.log`

**Related links**

Identity certificate renewal on page 323

# Chapter 15: Resources

## Documentation

See the following related documents at http://support.avaya.com:

| Title | Use this document to: | Audience |
|---|---|---|
| Overview | | |
| *Avaya Aura® Session Manager Overview and Specification* | See characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security, and licensing requirements of the Avaya Aura® Session Manager. | People who want to gain a high-level understanding of the Avaya Aura® Session Manager features, functions, capacities, and limitations. |
| *Avaya Aura® Communication Manager Feature Description and Implementation* | See characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security, and licensing requirements of the Avaya Aura® Communication Manager. | People who want to gain a high-level understanding of the Avaya Aura® Communication Manager features, functions, capacities, and limitations. |
| Avaya IP Office™ Platform Feature Description | See information about the feature descriptions. | People who perform system administration tasks. |
| Avaya IP Office™ Platform Solution Description | See information about how the products and services interoperate with this solution. | People who want to gain a high-level understanding of the IP Office features, functions, capacities, and limitations. |
| Implementing | | |
| *Deploying Avaya Aura® Session Manager* | See the installation procedures and initial administration information for Avaya Aura® Session Manager. | People who install, configure, and verify Avaya Aura® Session Manager on Avaya Aura® System Platform. |

*Table continues…*

| Title | Use this document to: | Audience |
|---|---|---|
| *Upgrading Avaya Aura® Session Manager* | See upgrading checklists and procedures. | People who perform upgrades of Avaya Aura® Session Manager. |
| *Deploying Avaya Aura® System Manager on System Platform* | See the installation procedures and initial administration information for Avaya Aura® System Manager. | People who install, configure, and verify Avaya Aura® System Manager on Avaya Aura® System Platform at a customer site. |
| IP Office SIP Telephone Installation Notes | See the installation procedures and initial administration information for IP Office SIP telephone devices. | People who install, configure and verify SIP telephone devices on IP Office. |
| Administering | | |
| *Administering Avaya Aura® Session Manager* | See information about performing Avaya Aura® Session Manager administration tasks, including how to use management tools, how to manage data and security, and how to perform periodic maintenance tasks. | People who perform Avaya Aura® Session Manager system administration tasks. |
| *Administering Avaya Aura® System Manager* | See information about performing Avaya Aura® System Manager administration tasks, including how to use management tools, how to manage data and security, and how to perform periodic maintenance tasks. | People who perform Avaya Aura® System Manager administration tasks. |
| Administering Avaya IP Office™ Platform with Manager | See information about short code configurations for the feature list | People who need to access IP Office features using short codes. |
| Administering Avaya IP Office™ Platform with Web Manager | See information about IP Office Web Manager administration tasks, including how to use the management tool, how to manage data and security, and how to perform maintenance tasks. | People who perform IP Office Web Manager administration tasks. |
| Maintaining | | |
| *Maintaining Avaya Aura® Session Manager* | See information about the maintenance tasks for Avaya Aura® Session Manager. | People who maintain Avaya Aura® Session Manager. |
| *Troubleshooting Avaya Aura® Session Manager* | See information for troubleshooting Avaya Aura® Session Manager, resolving alarms, replacing hardware, alarm codes, and event ID descriptions. | People who troubleshoot Avaya Aura® Session Manager. |

*Table continues…*

| Title | Use this document to: | Audience |
|---|---|---|
| Using IP Office System Status | See information about the maintenance tasks for System Status Application. | People who maintain System Status Application. |
| Using IP Office System Monitor | See information about the maintenance tasks for SysMonitor. | People who maintain SysMonitor. |

# 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.<br>Value operation:<br>• 0: The tag is not included.<br>• 1: The tag is included. |
| A | | |
| ACOUSTIC_EXPOSURE_PROTECT_MODE_DEFAULT | Off | Specifies the long-term acoustic exposure protection mode default setting.<br>Value operation:<br>• Off<br>• Dynamic<br>• 4 hours<br>• 8 hours<br>**Note:**<br>Avaya J129 IP Phone does not support long-term acoustic exposure protection. |
| ADMIN_LOGIN_ATTEMPT_ALLOWED | 10 | Specifies the allowed number of failed attempts to enter the access code before the local or craft procedures gets locked. Valid values are from 1 to 20. |
| ADMIN_LOGIN_LOCKED_TIME | 10 | Specifies the duration for lockout when a user reaches the maximum attempts limit for accessing the Administration menu.<br>Valid values are from 5 minutes to 1440 minutes. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ADMIN_PASSWORD | 27238 | Specifies an access code for accessing the Admin menu.<br>Valid values are from 6 to 31 alphanumeric characters including upper case, lower case characters and special characters. However, double quote character (“) cannot be used for a value of this parameter.<br>**Note:**<br>• If this parameter length is set below 6 or above 31 alphanumeric characters, then the parameter is treated as not defined.<br>• If this parameter is set in the `46xxsettings.txt` file, then it replaces PROCPSWD parameter.<br>• If you set ADMIN_PASSWORD in the Avaya Aura® System Manager you require at least Avaya Aura® System Manager 7.1.0.<br>• Setting this parameter through PPM is more secure because this file can usually be accessed and read by anyone on the network. Setting the value in this file is intended primarily for configurations with versions of phone or if server software that do not support setting this value from the server. |
| AGCHAND | 1 | Specifies the status of Automatic Gain Control (AGC) for the handset.<br>Value operation:<br>• 0: Disables AGC for the handset.<br>• 1: Enables AGC for the handset. |
| AGCHEAD | 1 | Specifies the status of Automatic Gain Control (AGC) for the headset.<br>Value operation:<br>• 0: Disables AGC for the headset.<br>• 1: Enables AGC for the headset. |
| AGCSPKR | 1 | Specifies the status of Automatic Gain Control (AGC) for the speaker.<br>Value operation:<br>• 0: Disables AGC for the speaker.<br>• 1: Enables AGC for the speaker. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| AGTGREETINGSTAT | 0 | Specifies whether the Agent Greetings feature is enabled or not.<br>Value operation:<br>• 0: Disabled<br>• 1: enabled |
| AGTGREETLOGOUTDEL | 5 | Specifies whether the phone deletes agent greeting messages upon the agent logout.<br>• 0: The phone deletes agent greeting messages.<br>• 1: The phone saves agent greeting messages. |
| AGENTGREETINGSDELAY | 0 | Specifies delat time in milliseconds between call pickup and agent greeting message playback start.<br>Valid values are 0-3000 |
| ALLOW_DND_SAC_LINK_CHANGE | 0 | Specifies if the user is allowed to change the DND and SAC button link. If the change is allowed, the menu to set the DND and SAC link is displayed.<br>Value operation:<br>• 0: Do not allow a user to change default behavior (Default).<br>• 1: Allow a user to change default behavior.<br>**Important:**<br>This parameter is not supported from firmware version 4.0.8.0 and later. For firmware version 4.0.8.0 and later, the parameter DND_SAC_LINK provides the enhanced functionality.<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |
| ALWAYS_FAVORITES_FOR_BUTTON_MODULES | 0 | Specifies whether the Always Favorites on Button Module feature is enabled or not.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled |

*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. This Application Header context relies on SHORT_FORM_USER_ID and DISPLAY_NAME to display the Application Header line context appropriately.<br>Value operation:<br>0: appearances context will not be shown on the Application Header Line (default)<br>1: appearances context will be shown on the Application Header Line<br>If this parameter is enabled but both SHORT_FORM_USER_ID and DISPLAY_NAME are null, then the userid of the registered SIP user will be displayed.<br>If the Agent login and logout feature is enabled on Avaya J159 IP Phone, the value for this parameter must be 0.<br>**Note:**<br>Avaya J129 IP Phone does not support this parameter. |
| APPNAME_IN_USE | Null | Used to check which firmware version is installed on the phone to perform a corresponding action, for example:<br>`IF $APPNAME_IN_USE SEQ 4.0.2.0.11 GOTO CROSSGRADE` |
| ASTCONFIRMATION | 60 | Specifies the number of seconds that the phone waits to validate an active subscription when it subscribes to the avaya-cm-feature-status package.<br>Valid values are 16 through 3600. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| AUDASYS | 3 | Specifies the audible alerting setting for the phone.<br>Value operation:<br>• 0: Turns off audible alerting. User cannot adjust ringer volume.<br>• 1: Turns on audible alerting. User can adjust ringer volume, but cannot turn off audible alerting.<br>• 2: Turns off audible alerting. User can adjust ringer volume and can turn off audible alerting.<br>• 3: Turns on audible alerting. User can adjust ringer volume and can turn off audible alerting.<br>**Note:**<br>Avaya J129 IP Phone does not support this parameter. |
| AUDIOENV | 0 | Specifies the audio environment index and enables you to customize the phone's audio performance.<br>Valid values are 0 through299.<br>This parameter affects settings for AGC dynamic range and handset noise reduction thresholds. Always consult Avaya before changing this parameter. |
| AUDIOSTHD | 0 | Specifies the level of sidetone in the headset.<br>Value operation:<br>• 0: Normal level for most users<br>• 1: Three levels softer than normal<br>• 2: Off, inaudible<br>• 3: One level softer than normal<br>• 4: Two levels softer than normal<br>• 5: Four levels softer than normal<br>• 6: Five levels softer than normal<br>• 7: Six levels softer than normal<br>• 8: One level louder than normal<br>• 9: Two levels louder than normal<br>**Note:**<br>Avaya J129 IP Phone does not support this parameter. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| AUDIOSTHS | 0 | Specifies the level of sidetone in the handset.<br>Value operation:<br>• 0: Normal level for most users<br>• 1: Three levels softer than normal<br>• 2: Off, Inaudible<br>• 3: One level softer than normal<br>• 4: Two levels softer than normal<br>• 5: Four levels softer than normal<br>• 6: Five levels softer than normal<br>• 7: Six levels softer than normal<br>• 8: One level louder than normal<br>• 9: Two levels louder than normal |
| AUTH | 0 | Specifies whether the script files are downloaded from an authenticated server over an HTTPS link.<br>Value operation:<br>• 0: Optional<br>• 1: Mandatory<br>To revert the configured value of 1 to the default one, reset the phone to defaults. |
| AUTHCTRLSTAT | 0 | Specifies if the enhanced debugging capabilities can be activated from the SSH server by the Avaya technicians only.<br>Value operation:<br>• 0: Enhanced debugging capabilities are disabled.<br>• 1: Enhanced debugging capabilities are enabled.<br>The parameter must be set to 1 only for the debugging period by Avaya technicians. Set the parameter back to 0 when the debugging period completes. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| AUTO_SELECT_ANY_IDLE_APPR | 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.<br>Value operation:<br>• 0: Disabled. Both parameters AUTO_SELECT_ANY_IDLE_APPR and AUTO_SELECT_ANY_IDLE_APPR are set to 0.<br>• 1: Enabled. The parameter CONF_TRANS_ON_PRIMARY_APPR is set to 0.<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |
| AUTO_UNMUTE | 0 | Specifies whether the call is not in a muted state when the transducer is changed. This feature is applied on all types of calls.<br>Value operation:<br>• 0: Disabled. Call is in mute state.<br>• 1: Enabled. Call is not in mute state.<br>**Note:**<br>Only Avaya J159 IP Phone and Avaya J169/J179 IP Phone supports this feature. |
| AUTOMATIC_UPDATE_DAYS | Sun | Specifies the days of automatic update.<br>This parameter is applicable only when AUTOMATIC_UPDATE_POLICY is set to value 2 or 3.<br>Mon, Tue, Wed, Thu, Fri, Sat, Sun for weekly update.<br>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.<br>The phone uses the default value if you set invalid values.<br>Example for weekly update SET AUTOMATIC_UPDATE_DAYS "Sun"<br>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.<br><br>AUTOMATIC_UPGRADE_INSTALL_DATE_TIME is applicable if AUTOMATIC_UPDATE_POLICY is set to 1, 2, or 3.<br><br>The format is YYYY-MM-DDThh:mm, where:<br><br>• YYYY is 4 digit numeric value for year, MM is 2 digit numeric value for month<br><br>• DD is 2 digit numeric value for date, which is 1 to 31<br><br>• T is the time separator<br><br>• hh is 2 digit numeric value for hours of the day which is 00 to 23<br><br>• mm is 2 digit numeric value for minutes of the hour, which is 00 to 59<br><br>For example: SET AUTOMATIC_UPGRADE_INSTALL_DATE_TIME 2015-04-12T23:20<br><br>Note that this parameter applies to the phone local time as defined by the following parameters:<br><br>• GMTOFFSET<br><br>• DAYLIGHT_SAVING_SETTING_MODE<br><br>• DSTOFFSET<br><br>• DSTSTART<br><br>• 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.<br><br>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.<br><br>Value operation:<br><br>• 0: The phone does not display the reboot confirmation prompt, instead it updates the phone directly.<br><br>• 1: The phone displays the reboot confirmation prompt. |
| AUTOMATIC_UPDATE_POLICY | 0 | Specifies the automatic update frequency.<br><br>Value operation:<br><br>• 0: Disabled<br><br>• 1: Daily<br><br>• 2 : Weekly<br><br>• 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.<br><br>Each phone picks a random time between this specified window.<br><br>The time is in 24hr format.<br><br>For example SET AUTOMATIC_UPDATE_WINDOW "23,0"<br><br>Sets one hour window from 11 PM to 00 AM for the automatic update. |
| AWAY_TIMER | 1 | Controls whether the phone reports an away state.<br><br>Value operation:<br><br>• 0: Disabled<br><br>• 1: Enabled (default). The phone automatically reports an away state |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| 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.<br><br>The range is 1-1500 minutes. |
| BACKGROUND_IMAGE | Null | Specifies custom background images that can be loaded from the provisioning server.<br><br>Phone supports up to 5 background images with the following limitation:<br><br>• jpeg format files are supported until software version 4.0.11 and earlier.<br><br>From software version 4.0.12 and later, only jpg format files are supported.<br><br>• The maximum file size is 256 KB.<br><br>• The file names are case sensitive.<br><br>Avaya J169/J179 IP Phone, Avaya J159 IP Phone, screen resolution is 320 pixels x 240 pixels. Avaya J169/J179 IP Phone color depth is 16 bits and Avaya J189 IP Phone. Avaya J169/J179 IP Phone phones support grayscale color spaces and other color display phones support yCbCr color spaces.<br><br>The files shall be stored in the same directory defined by HTTPDIR / TLSDIR.<br><br>Example: SET BACKGROUND_IMAGE [xxx.jpg] |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| BACKGROUND_IMAGE_DISPLAY | Null | Specifies the background image to be displayed on the phone.<br>Value operation:<br>• 0: To select default image 1.<br>• 1: To select default image 2.<br>• 2: To select default image 3.<br>• 3: To select default image 4.<br>• 4: To select default image 5.<br>• 5: To select default image 6.<br>• 6: To select default image 7.<br>Note that, If BACKGROUND_IMAGE_SELECTABLE is set to 1 then the end user may override this setting.<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |
| BACKGROUND_IMAGE_DISPLAY_JEM | Null | Specifies the background image to be displayed on the Avaya J100 Expansion Module.<br>The default value is empty. The value is separated by commas without any intervening spaces.<br>To select one of the seven built-in default images, need to specify a value from 0 to 6.<br>• 0: To select default image 1.<br>• 1: To select default image 2.<br>• 2: To select default image 3.<br>• 3: To select default image 4.<br>• 4: To select default image 5.<br>• 5: To select default image 6.<br>• 6: To select default image 7.<br>**Note:**<br>Note: If the parameter is not set, then a Avaya J100 Expansion Module background image must be set to default Avaya device image. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| BACKGROUND_IMAGE_JEM | Null | Specifies a comma-separated list of background images for the Avaya J100 Expansion Module display.<br>The value is separated by commas without any intervening spaces.<br>Avaya J100 Expansion Module supports up to 5 background images with the following limitation:<br>• Only jpg format files are supported.<br>• The maximum file size is 256 KB.<br>• The file names are case sensitive.<br>• The color depth is limited to 16 bits.<br>The Avaya J100 Expansion Module has a resolution of 272 x 480 pixels.<br>The files must be stored in the directory specified by HTTPDIR or TLSDIR. |
| BACKGROUND_IMAGE_JEM_FOLLOW_PRIMARY | 1 | Specifies whether the Avaya J100 Expansion Module background image always follows the primary display or can have a separate background image.<br>The options are:<br>• 0: You can configure a separate background image for the Avaya J100 Expansion Module background.<br>• 1: Avaya J100 Expansion Module background image always follows the primary display. |
| BACKGROUND_IMAGE_SELECTABLE | 1 | Allows the end user to select background images.<br>Value operation:<br>• 0: The user can not use a background images from the phone UI.<br>• 1: The user can select a background images from the phone UI.<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| BACKGROUND_IMAGE_SELECTABLE_JEM | 1 | Specifies whether the user can select a background image.<br>The options are:<br>• 0: The end user is not allowed to choose the Avaya J100 Expansion Module background image. The value set by an administrator is used.<br>• 1: The end user is allowed to choose the Avaya J100 Expansion Module background image. |
| 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:<br>• jpeg format files are supported until software version 4.0.11 and earlier.<br>From software version 4.0.12 and later, only jpg format files are supported.<br>• The maximum file size is 256 KB.<br>• The file names are case sensitive.<br>Example:<br>background_example1.jpg,background_example2.jpeg<br>**Note:**<br>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.<br>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.<br>Value operation:<br>• 0: The user can not use a background images from the phone UI.<br>• 1: The user can select a background images from the phone UI.<br>This parameter overrides the value configured using BACKGROUND_IMAGE_DISPLAY_SECONDARY parameter<br>**Note:**<br>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.<br>Value operation:<br>• 0: To set Backlight Timer value from the `46xxsettings.txt` file.<br>• 1: To set Backlight Timer value according to user settings.<br>**Note:**<br>Only Avaya J169/J179 IP Phone supports this feature. |
| BAKLIGHTOFF | 120 | Specifies the number of minutes of idle time after which the display backlight will be turned off.<br>Phones with gray-scale displays do not completely turn backlight off, they set it to the lowest non-off level.<br>Valid values are 0 through 999.<br>A value of 0 means that the display backlight will not be turned off automatically when the phone is idle.<br>For ENERGY STAR compliance on applicable phones, a value of 20 is recommended. |
| BLOCK_CERTIFICATE_WILDCARDS | 0 | Specifies whether the endpoint will accept server identity certificates with wildcards.<br>Value operation:<br>• 0: Accept wildcards in certificate.<br>• 1: Do not accept wildcards in certificates. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| BLUETOOTHSTAT | 1 | Specifies whether the user is given an option to enable the Bluetooth.<br>Value operation:<br>• 0: Bluetooth is disabled and the user is not given an option to enable it.<br>• 1: The user is given an option to enable the Bluetooth.<br>**Note:**<br>This parameter is supported only in Avaya J159 IP Phone, Avaya J179 IP Phone, and Avaya J189 IP Phone |
| BRANDING_VOLUME | 5 | Specifies the volume level at which the Avaya audio brand is played.<br>Value operation:<br>• 8: 9db above nominal<br>• 7: 6db above nominal<br>• 6: 3db above nominal<br>• 5: nominal<br>• 4: 3db below nominal<br>• 3: 6db below nominal<br>• 2: 9db below nominal<br>• 1:12db below nominal<br>• 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 |
|---|---|---|
| BUTTON_MAPPINGS | Null | Specifies a list of Button and Status pairs that change the operation of some of the buttons on the phone.<br>Button and Status pairs are separated by commas without any intervening spaces.<br>Valid button values are Forward, Speaker, Hookswitch, and Headset.<br>Valid Status values are na and cc-release.<br>Value operation:<br>• na: The corresponding button is disabled.<br>• cc-release: Button invokes the cc-release feature.<br>• null: All buttons operate normally. |
| C | | |
| CALL_DECLINE_POLICY | 0 | Specifies whether the user can decline the incoming call. You can enable and disable the feature using the following options:<br>The options are:<br>• **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.<br>• **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.<br>• **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. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| 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.<br>Value operations:<br>• 0: First user to have forwarded is shown as the Forwarded By User.<br>• 1: Last user to have forwarded is shown as the Forwarded By User.<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |
| CALLFWDDELAY | 1 | Sets the number of ring cycles before the call is forwarded to the forward or coverage address. The default delay is one ring cycle. |
| CC_INFO_TIMER | 8 | Specifies the duration, in hours, of the subscription to the SIP CC-Info event package.<br>Valid values are 0 through 24. The default value is 8.<br>When the value is 0, the subscription doesn't expire. Use value 0 for the Service Observer feature through CTI. |
| 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.<br>Value operation:<br>• 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. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| CLDISPCONTENT | 1 | Specifies whether the name, the number, or both will be displayed for Call Log entries.<br>Value operation:<br>• 0: Both the name and the number will be displayed.<br>• 1: Only the name will be displayed.<br>**Note:**<br>Avaya J129 IP Phone and Avaya J139 IP Phone do not support this parameter. |
| CODEC_PRIORITY | OPUS,G722,G711U,G711A,G726,G729 | Specifies the priority order for all codecs, supported by the phones.<br>Valid value is a string of correct codec names, separated by a comma with no blank spaces. For example:<br>`SET CODEC_PRIORITY OPUS,G722,G711U,G711A,G726,G729`<br>If values are entered incorrectly or the phone does not support the listed codec, the value is ignored. |

*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.<br><br>Value operation:<br><br>• 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 bidged call extension is not available, the setup initiated on a bridged call appearance will be denied.<br><br>• 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.<br><br>**Note:**<br><br>Avaya J129 IP Phone does not support this feature. |
| CONFERENCE_FACTORY_URI | Null | Specifies the URI for Avaya Aura Conferencing.<br><br>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.<br><br>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.<br><br>The value can contain 0 to 255 characters. The default value is null. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| CONFERENCE_TYPE | 1 | Determines the selection of the Conference Method.<br>Value operation:<br>• 0: Local conferencing is supported based on sipping services.<br>• 1: Server based conferencing is supported.<br>• 2: Click-to conference server based conferencing is supported.<br>If the parameter is set to a value that is outside the range then default value is selected. |
| CONFIG_SERVER_SECURE_MODE | 1 | Specifies whether HTTP or HTTPS is used to access the configuration server.<br>Value operation:<br>• 0: HTTP<br>• 1: HTTPS<br>• 2: Use HTTPS if SIP transport mode is TLS, otherwise use HTTP. |
| CONTACT_NAME_FORMAT | 0 | Specifies how contact names are displayed.<br>Value operation:<br>• 0: The name format is Last name, First name.<br>• 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.<br>Valid values are 4 through 3600. |
| CONNECTION_REUSE | 1 | Specifies whether the phone will use two UDP, TCP, or TLS connection (for both outbound and inbound) or one UDP, TCP, or TLS connection.<br>Value operation:<br>• 0: Disabled. The phone opens outbound connection to the SIP Proxy and listening socket for inbound connection from SIP proxy in parallel.<br>• 1: Enabled. The phone does not open a listening socket and will maintain and re-use the sockets it creates with the outbound proxies.<br>**Note:**<br>On Avaya J129 IP Phone, only 1 is supported. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| COUNTRY | USA | Used for network call progress tones.<br>• For Argentina use keyword Argentina.<br>• For Australia use keyword Australia.<br>• For Brazil use keyword Brazil.<br>• For Canada use keyword USA.<br>• For France use keyword France.<br>• For Germany use keyword Germany.<br>• For Italy use keyword Italy.<br>• For Ireland use keyword Ireland.<br>• For Mexico use keyword Mexico.<br>• For Spain use keyword Spain.<br>• For United Kingdom use keyword UK.<br>• For United States use keyword USA.<br>Country names with spaces must be enclosed in double quotes. |
| CURRENT_LOGO | Null | Specifies if custom logo or wallpaper is selected for display.<br>The CURRENT_LOGO is used in the following cases:<br>• The phone is not registered to Avaya Aura® Session Manager.<br>• The phone is registered to Avaya Aura® Session Manager and<br>- there is no information stored for the current logo file for this specific user, and<br>- there is no support of Profile Settings in the Endpoint Template. This is supported by Avaya Aura® System Manager 6.3.8 and later.<br>**Note:**<br>Only Avaya J169/J179 IP Phone supports this parameter. |
| CUSTOMIZATION_MODE | 2 | Specifies the customization mode.<br>Value operation:<br>• 0: Blocked<br>• 1: Limited<br>• 2: Full |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| D | | |
| 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.<br>• Use %d for day of month<br>• Use %m for month in decimal format.<br>• Use %y for year without century (e.g., 07).<br>• Use %Y for year with century (e.g., 2007).<br>Any character not preceded by % is reproduced exactly.<br>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.<br>Value operation:<br>• 0: Daylight saving time not activated<br>• 1: Daylight saving time is activated. Time set to DSTOFFSET.<br>• 2: Activates automatic daylight savings adjustment as specified by DSTSTART and DSTSTOP. |
| DELETE_DES_CERT | 0 | Specifies whether the installed identity certificate for profile DES will be deleted.<br>Valid values:<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed. |
| DELETE_MY_CERT | 0 | Specifies whether the installed identity certificate, using SCEP or PKCS12 file download, will be deleted.<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed. |
| DELETE_PKCS12_CERT | 0 | Specifies whether the installed identity certificate for profile PKCS12#1 will be deleted.<br>Valid values:<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed.<br>When parameter value is 1, phone removes identity certificate for PKCS#1 profile. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| DELETE_PKCS12_2_CERT | 0 | Specifies whether the installed identity certificate for profile PKCS12#2 will be deleted.<br>Valid values:<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed.<br>When parameter value is 1, phone removes identity certificate for PKCS12#2 profile. |
| DELETE_PKCS12_3_CERT | 0 | Specifies whether the installed identity certificate for profile PKCS12#3 will be deleted.<br>Valid values:<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed.<br>When parameter value is 1, phone removes identity certificate for PKCS12#3 profile. |
| DELETE_SCEP_CERT | 0 | Specifies whether the installed identity certificate for profile SCEP#1 will be deleted.<br>Valid values:<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed.<br>When parameter value is 1, phone removes identity certificate for SCEP#1 profile. |
| DELETE_SCEP_2_CERT | 0 | Specifies whether the installed identity certificate for profile SCEP#2 will be deleted.<br>Valid values:<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed.<br>When parameter value is 1, phone removes identity certificate for SCEP#2 profile. |
| DELETE_SCEP_3_CERT | 0 | Specifies whether the installed identity certificate for profile SCEP#3 will be deleted.<br>Valid values:<br>• 0: Installed identity certificate remains valid.<br>• 1: Installed identity certificate is removed.<br>When parameter value is 1, phone removes identity certificate for SCEP#3 profile. |

*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.<br>Value operation:<br>• 0: DES discovery is disabled and can only be restored with Reset to Defaults<br>• 1: DES discovery is disabled<br>• 2: DES discovery is enabled<br>• 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.<br>**Note:**<br>DHCPv4 is always enabled in IPv4 only and dual mode. DHCPv4 is disabled in IPv6 only mode.<br>Value operation:<br>• 1: run DHCPv4 only.<br>• 2: run DHCPv6 only.<br>• 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.<br>Value operation:<br>• 0: Continue using the address in an extended rebinding state.<br>• 1: Immediately stop using the address. |
| 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.<br>Value operation:<br>• 0: DHCPv6 enters proprietary extended rebinding state (continue to use IPv6 address, if DHCPv6 lease expires).<br>• 1: DHCPv6 complies with IETF RFC 8415 standard (immediately release IPv6 address, if DHCPv6 lease expires). |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| DIALPLAN | Null | Specifies the dial plan used in the phone.<br>Dialplan accelerates dialing by eliminating the need to wait for the INTER_DIGIT_TIMEOUT timer to expire.<br>The value can contain 0 to 1023 characters. The default value is null. |
| 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.<br>Valid value is a string of alphanumeric rules. If a rule uses incorrect characters, the phone ignores it.<br>The preferred way of configuring this parameter is through the web interface. |
| DIRUSERNAME | Null | Specifies the LDAP client username.<br>The following characters are allowed:<br>• 0–9<br>• a-z<br>• A-Z<br>The preferred way of configuring this parameter is through the web interface.<br>**Note:**<br>Avaya J129 IP Phone does not support this parameter. |
| DIRPASSWORD | Null | Specifies the LDAP client password.<br>The following characters are allowed:<br>• 0–9<br>• a-z<br>• A-Z<br>The preferred way of configuring this parameter is through the web interface.<br>**Note:**<br>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.<br>Value operation:<br>• 0: Use TCP<br>• 1: Establish TLS connection using the STARTTLS extended operation<br>• 2: Establish TLS connection using the Secure LDAP protocol (LDAPS)<br>For example, `SET DIRSECURE 1`<br>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.<br>The LDAPS protocol uses a port different from LDAP. The value for DIRSRVRPRT needs to correspond to server port for the LDAPS connection.<br>**Note:**<br>Avaya J129 IP Phone does not support this parameter. |
| DIRAUTHTYPE | 1 | Specifies the kind of authentication that is used if the value of the DIRUSERNAME parameter is not null.<br>Value operation:<br>• 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.<br>• 1:-Simple LDAP Authentication and Security Layer (SASL).<br>If a connection is established over TLS (DIRSECURE is set to 1 or 2), DIGEST-MD5 or PLAIN authentication mechanisms are supported.<br>If the connection established over TCP (DIRSECURE is set to 0) DIGEST-MD5 is the only supported mechanism.<br>**Note:**<br>Avaya J129 IP Phone does not support this parameter. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| DIRENABLED_PLATFORM | 0 | Determines whether the LDAP directory search is enabled on the phone.<br>Value operation:<br>• 0: No<br>• 1: Yes<br>**Note:**<br>Avaya J129 IP Phone does not support this parameter. |
| DIRNAME_FIELDS | cn | Specifies the attributes and their order, shown in the search results. Users can view other attributes, pressing the **Details** soft key.<br>The attributes, specified in this parameter must be a subset of the attributes, specified in DIRNAME_FIELDS.<br>For example, `SET DIRNAME_FIELDS "cn,sn"`<br>In this example, each match on a search result list displays a last name and a first name.<br>**Note:**<br>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.<br>For example, `SET DIRNUMBER_FIELDS "telephoneNumber, mobile, DoD SIP URI"`<br>**Note:**<br>Avaya J129 IP Phone does not support this parameter. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| DIRSEARCH_FIELDS | cn,sn,telephone Number | 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.<br><br>When configuring this parameter, you must use attribute names that coincide with the selected LDAP server attribute names.<br><br>For example, `SET DIRSEARCH_FIELDS "givenName,mail,middle initials, telephoneNumber, sn,mobile, department, Rank, office,DoD SIP URI"`<br><br>**Note:**<br><br>Avaya J129 IP Phone does not support this parameter. |
| 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.<br><br>Value operation:<br><br>• 0: Use TCP<br><br>• 1: Use TLS<br><br>For example, `SET DIRSECURE 1`<br><br>**Note:**<br><br>Avaya J129 IP Phone does not support this parameter. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| DIRSHOW_FIELDS | cn,sn,telephone Number,Mail | Specifies LDAP detail show fields. The phone returns the attributes, specified in this parameter, for each match found for a search query.<br><br>You can use this parameter to map the specified LDAP keywords. This mapping defines the way the phone displays show fields.<br><br>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"`<br><br>In this example, the format is as follows:<br><br>`SET DIRSHOW_FIELDS "[LDAP Attributes]=[Field Names], [LDAP Attribute 1]=[Field Name1]"`<br><br>**Note:**<br><br>Avaya J129 IP Phone does not support this parameter. |
| DIRSRVR | Null | Specifies the IP address or a fully qualified domain name (FQDN) of the LDAP directory server.<br><br>The valid value is an IPv6, IPv4 address in the dotted decimal format or a FQDN.<br><br>For example, `SET DIRSRVR 192.168.161.54` or `SET DIRSRVR domain.com`<br><br>**Note:**<br><br>Avaya J129 IP Phone does not support this parameter. |
| DIRSRVRPRT | 389 | Specifies the port number for the LDAP directory server.<br><br>Valid values are positive integers from 1 to 65535.<br><br>For example, `SET DIRSFVFRT 389`<br><br>**Note:**<br><br>Avaya J129 IP Phone does not support this parameter. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| DIRTOPDN | Null | Specifies the LDAP search base.<br>For example, `SET DIRTOPDN "dc=global, dc=avaya, dc=com"`<br>**Note:**<br>Avaya J129 IP Phone does not support this parameter. |
| 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.<br>Local contact field names can be assigned from the following: "firstName"<br>• "nickname"<br>• "URI"<br>• "extension"<br>• "email"<br>• "department"<br>• "zipCode"<br>• "country"<br>for number types:<br>• "work"<br>• "home"<br>• "mobile"<br>• "other"<br>**Note:**<br>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.<br>Valid value is a text string. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| DISCOVER_AVAYA_ENVIRONMENT | 1 | Specifies dynamic feature set discovery<br>Value operation:<br>• 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.<br>• 0: The phone operates in a mode where AST features are not available.<br>**Note:**<br>Set the parameter to 0 for IP Office environment. |
| DIR_LDAP_DESCRIPTION | “LDAP Directory | Specifies a custom label to be used for the LDAP directory in the Contacts application.<br>Valid value is a text string.<br>**Note:**<br>Avaya J129 IP Phone does not support this parameter. |
| DISPLAY_NAME | Null | Specifies the custom Caller ID displayed on the call appearance for the host and the remote phone.<br>Valid value is a text string of non-ASCI symbols, up to 255 characters long. For example:<br>SET DISPLAY_NAME "John Smith"<br>The following symbols are not valid values: ";<>/&<br>**Note:**<br>IP Office does not support this parameter. |
| DISPLAY_SSL_VERSION | 0 | Specifies whether OpenSSL and OpenSSH versions are displayed in the **Administration** menu.<br>Value operation:<br>• 0: OpenSSL and OpenSSH versions are not displayed.<br>• 1: OpenSSL and OpenSSH versions are displayed. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| DND_SAC_LINK | 0 | Specifies whether to activate the SendAllCall when user enables DoNotDisturb.<br>The value of this parameter is used if the ALLOW_DND_SAC_LINK_CHANGE is set to 0<br>Value operation:<br>• 0: Do not activate the SendAllCall when user enables DoNotDisturb (default).<br>• 1: Activate the SendAllCall when user enables DoNotDisturb.<br>• 2: Activate the SendAllCall when user enables DoNotDisturb and vice-versa.<br>• 3: Forced do not activate the SendAllCall when user enables DoNotDisturb.<br>• 4: Forced activate the SendAllCall when user enables DoNotDisturb.<br>• 5: Forced activate the SendAllCall when user enables DoNotDisturb and vice-versa.<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |
| DNSSRVR | Null | Specifies a character string that will be appended to parameter values that are specified as DNS names, before the name is resolved.<br>The value can contain 0 to 255 characters. The default value is null.<br>This parameter can be set through:<br>• DHCP<br>• The settings file.<br>Setting this parameter through the settings file overwrites any values set through DHCP. |

*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.<br>The value can contain 0 to 255 characters. The default value is null.<br>This parameter can be set through:<br>• DHCP<br>• The settings file.<br>Setting this parameter through the settings file overwrites any values set through DHCP. |
| DOT1X | 0 | Specifies the 802.1X pass-through operating mode.<br>Pass-through is the forwarding of EAPOL frames between the phone's ethernet line interface and its secondary (PC) ethernet interface<br>Value operation:<br>• 0: EAPOL multicast pass-through enabled without proxy logoff.<br>• 1: EAPOL multicast pass-through enabled with proxy logoff.<br>• 2: EAPOL multicast pass-through disabled. |
| DOT1XEAPS | MD5 | Specifies the authentication method to be used by 802.1X.<br>Valid values are:<br>• MD5<br>• TLS<br>• PEAP<br>If you select MD5 or PEAP, configure the parameters FORCE_DOT1XID and FORCE_DOT1XPSWD, else the phone prompts you to provide the inputs for DOT1XID and DOT1XPSWD on the administration menu.<br>If you select PEAP, the phone only supports PEAP Phase 2 authentication method MSCHAPv2.<br>If you select TLS, configure the parameter FORCE_DOT1XID_TLS, else the phone prompts you to provide the input for DOT1XID_TLS on the administration menu. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| DOT1XSTAT | 0 | Specifies the 802.1X supplicant operating mode.<br>Value operation:<br>• 0: Supplicant disabled.<br>• 1: Supplicant enabled, but responds only to received unicast EAPOL messages.<br>• 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.<br>Valid values are from 0 to 63.<br>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.<br>Valid values are from 0 to 63. |
| DSCPAUD_FO | 41 | Specifies the DSCP value for flash Override precedence or priority level voice call.<br>Valid values are from 0 to 63.<br>**Note:**<br>Only Avaya J129 IP Phone supports this feature. |
| DSCPAUD_IM | 45 | Specifies the DSCP value for immediate precedence or priority level voice call.<br>Valid values are from 0 to 63.<br>**Note:**<br>Only Avaya J129 IP Phone supports this feature. |
| DSCPAUD_PR | 47 | Specifies the DSCP value for priority precedence or priority level voice call.<br>Valid values are from 0 to 63.<br>**Note:**<br>Only Avaya J129 IP Phone supports this feature. |
| DSCPMGMT | 16 | Specifies the DSCP value for OA&M management packet.<br>Valid values are from 0 to 63.<br>**Note:**<br>Only Avaya J129 IP Phone supports this feature. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| DSCPSIG | 34 | Specifies the layer 3 Differentiated Services (DiffServ) Code Point for signaling frames generated by the phone.<br>Valid values are 0 through 63.<br>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.<br>Valid values are 0, 1, or 2. The default value is 1. |
| DSTSTART | 2SunMar2L | Specifies when to apply the offset for daylight savings time.<br>The date and time for applying the offset can be set in the following formats:<br>• `odddmmmht`: for example, `2SunMar2L` which corresponds to the second Sunday in March at 2 AM local time;<br>• `Dmmmht`: for example, `10Mar5L` which corresponds to March 10 at 5 AM local time. |
| DSTSTOP | 1SunNov2L | Specifies when to stop applying the offset for daylight savings time.<br>You can set the date and time when the offset is stopped in the following formats:<br>• `odddmmmht`: for example, `1SunNov2L` which corresponds to the first Sunday in November at 2 AM local time;<br>• `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.<br>Valid values are 96 through 127. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| DUAL_IPPREF | 4 | DUAL_IPPREF controls the following:<br>• The selection of SSON either from DHCPv4 or DHCPv6 server, when phone is in dual mode.<br>• Whether an IPv4 or IPv6 addresses returned by DNS would be tried first during dualmode operation.<br>DHCP clients use DUAL_IPPREF to decide which SSON configuration attributes to apply for DHCPv4 / DHCPv6 interworking in dual mode.<br>Value operation:<br>• 4: IPv4 is preferred.<br>• 6: IPv6 is preferred. |
| 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.<br>This parameter is supported by only Avaya J129 IP Phone.<br>Value operation:<br>• 0: EEE is disabled on both PHY1 and PHY2.<br>• 1; EEE is enabled on both PHY1 and PHY2. |
| ELD_SYSNUM | 1 | Controls whether Enhanced Local Dialing algorithm will be applied for System Numbers-Busy Indicators and Auto Dials.<br>Value operation:<br>• 0: Disable ELD for System Numbers<br>• 1: Enable ELD for System Numbers<br>**Note:**<br>Avaya J139 IP Phone does not support Busy Indicator feature. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ENABLE_3PCC_ENVIRONMENT | 1 | Specifies that the phone is working in the Third-party call control setup environment.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled<br>Set the parameter to 0 for Avaya Aura® and IP Office environment. |
| ENABLE_NIGHT_MODE | 0 | Specifies whether the Night mode soft key is available on the phone UI.<br>Value operation:<br>• 0: Do not allow<br>• 1: Allow<br>**Note:**<br>Only Avaya J179 IP Phone supports Night mode feature. |
| ENABLE_AVAYA_ENVIRONMENT | 1 | Specifies whether the phone is configured to be used in an Avaya (SES) or a third-party proxy environment.<br>Value operation:<br>• 0: Configured for 3rd party proxy with SIPPING 19 features.<br>• 1: Configured for Avaya environment with AST features and PPM. |
| ENABLE_BLIND_TRANSFER | 1 | Specifies that whether the blind transfer is enabled or not.<br>Value operation:<br>• 0: Disabled.<br>• 1: Enabled.<br>Avaya J129 IP Phone does not support this feature. |
| ENABLE_CALL_LOG | 1 | Specifies if call logging and associated menus are available on the phone.<br>Value operation:<br>• 0: No<br>• 1: Yes |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ENABLE_CONTACTS | 1 | Specifies if the contacts application and associated menus are available on the phone.<br>Value operation:<br>• 0: No. The phone disables the **Contacts** option on the interface.<br>• 1: Yes<br>**Note:**<br>The parameter is set to 1 in IP Office 10.1 or later. In previous releases it is set to 0. |
| 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.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled |
| ENABLE_EARLY_MEDIA | 1 | Specifies if the phone sets up a voice channel to the called party before the call is answered.<br>Value operation:<br>• 0: No<br>• 1: Yes<br>Setting this parameter to 1 can speed up call setup. |
| ENABLE_EXCHANGE_REMINDER | 0 | Specifies whether or not exchange reminders will be displayed.<br>Value operation:<br>• 0: Not displayed<br>• 1: Displayed<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ENABLE_FEATURE_INVOCATION_TARGET_SELECTION | 0 | This parameter is used to enable or disable the feature target selection.<br>The options are:<br>• 0: Disabled. This feature is disabled by default. The user must manually enter the extension number.<br>• 1: Enable the feature target selection. The user can enter the destination number using dial, contacts, recents, and phone button. The user can also use the browser soft key, autodial, busy indicator and team line keys to select the destination number. |
| ENABLE_G711A | 1 | Specifies if the G.711 a-law codec is enabled.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled |
| ENABLE_G711U | 1 | Specifies if the G.711 mu-law codec is enabled.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled |
| ENABLE_G722 | 1 | Specifies if the G.722 codec is enabled.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled |
| ENABLE_G726 | 1 | Specifies if the G.726 codec is enabled.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled |
| ENABLE_G729 | 1 | Specifies if the G.729A codec is enabled.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled without Annex B support (default).<br>• 2: Enabled with Annex B support. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| 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.<br>Value operation:<br>• 0: GDPR mode is disabled<br>• 1: GDPR mode is enabled<br>Avaya J129 IP Phone does not support this parameter. |
| 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.<br>Value operation:<br>• 0: Disabled, the phone does not send the HSTS header in HTTP response.<br>• 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.<br>Value operation:<br>• 0: The phone does not support IP Office (except in Avaya Aura failover mode).<br>• 1: The phone supports IP Office in a native environment.<br>• 2: The phone supports IP Office with additional features driven by the IP Office proxy.<br>Avaya J129 IP Phone supports value 0 and 1.<br>Avaya J139 IP Phone, Avaya J159 IP Phone and Avaya J169/J179 IP Phone support value 0 and 2. |
| ENABLE_MLPP | 0 | Specifies that whether the Multiple Level Precedence and Preemption (MLPP) is enabled or not.<br>Value operation:<br>• 0: Disabled.<br>• 1: Enabled. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ENABLE_MODIFY_CONTACTS | 1 | Specifies if the list of contacts and the function of the contacts application can be modified on the phone.<br>Value operation:<br>• 0: No<br>• 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.<br>Value operation:<br>• 0: No<br>• 1: Yes<br>**Note:**<br>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.<br>Value operation:<br>• 0: No, TLS is not required.<br>• 1: Yes, TLS is required.<br>**Note:**<br>A value of 0 is only intended for testing purposes. |
| 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.<br>Value operation:<br>• 0: OOD is not supported.<br>• 1: OOD is supported. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ENABLE_OPUS | 1 | Specifies if the OPUS codec capability of the phone is enabled or disabled.<br>Value operation:<br>• 0: Disabled.<br>• 1: Enabled OPUS wideband with bitrate of 20KBps.<br>• 2: Enabled OPUS narrowband with bitrate of 16KBps.<br>• 3: Enabled OPUS narrowband with bitrate of 12KBps.<br>• 4: Enabled OPUS super wideband.<br>**Note:**<br>Supported only in J189 phone. |
| 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.<br>Value operation:<br>• 0: Disabled. **Lock** soft key and feature button are not displayed.<br>• 1: Enabled. **Lock** soft key and feature button are displayed.<br>**Note:**<br>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.<br>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. |
| ENABLE_PPM_SOURCED_SIPPROXYSRVR<br>The parameter is only available in an Avaya Aura® environment. | 1 | Enables PPM as a source of SIP proxy server information.<br>Value operation:<br>• 0: Proxy server information received from PPM is not used.<br>• 1: Proxy server information received from PPM is not used. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ENABLE_PRECEDENCE_SOFTKEY | 1 | Specifies that whether the precedence soft key is enabled or not on the idle line appearances on Phone Screen.<br>Value operation:<br>• 0: Disabled.<br>• 1: Enabled.<br>**Note:**<br>Only Avaya J129 IP Phone supports this feature. |
| ENABLE_PRESENCE | 1 | Specifies if presence will be supported.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled<br>**Note:**<br>This parameter is set to 0 in IP Office environment. |
| 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<br>Value operation:<br>• 0: Embedded public CA certificates are only trusted when TRUSTCERTS is empty.<br>• 1: Embedded public CA certificates are always trusted. |
| ENABLE_RECORDING | 0 | Specifies if audio debug recording is enabled for users.<br>Value operation:<br>• 0: Audio debug recording is disabled.<br>• 1: Audio debug recording is enabled. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ENABLE_RANDOM_RTP_PORT | 0 | Specifies whether the random RTP port is enabled.<br>Value operation:<br>• 0: Even numbered RTP ports starting at RTP_PORT_LOW will be used for all calls.<br>• 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_RFC5922 | 1 | Specifies to enable or disable the RFC5922 certificate validation.<br>Value operation:<br>• 0: disable validation<br>• 1: enable validation |
| ENABLE_REDIAL | 1 | Specifies if **Redial** softkey is available.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| ENABLE_REDIAL_LIST | 1 | Specifies if the phone redials last number or displays list of recently dialed numbers.<br>Value operation:<br>• 0: Last number redial<br>• 1: User can select between the last redialled number and the redial list.<br>•<br>**Note:**<br>Avaya J129 IP Phone do not support this feature. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ENABLE_REMOVE_PSTN_ACCESS_PREFIX | 0 | Allows phone to perform digit manipulation during failure scenarios. This parameter allows removal of PSTN access prefix from the outgoing number.<br>Value operation:<br>• 0: PSTN access prefix is retained in the outgoing number.<br>• 1: PSTN access prefix is removed from the outgoing number. |
| ENABLE_SHOW_EMERG_SK | 2 | Specifies whether an **Emergency** softkey, with or without a confirmation screen, is displayed when the phone is registered. All emergency numbers are always supported.<br>Value operation:<br>• 0: **Emergency** softkey is not displayed.<br>• 1: **Emergency** softkey is displayed without a confirmation screen.<br>• 2: **Emergency** softkey is displayed with a confirmation screen.<br>**Note:**<br>The parameter is set to 0 for IP Office environment. |
| ENABLE_SHOW_EMERG_SK_UNREG | 2 | Specifies whether an **Emergency** softkey, with or without a confirmation screen, is displayed when the phone is not registered.<br>All emergency numbers will always be supported.<br>Value operation:<br>• 0: **Emergency** softkey is not displayed.<br>• 1: **Emergency** softkey is displayed without a confirmation screen.<br>• 2: **Emergency** softkey is displayed with a confirmation screen.<br>**Note:**<br>The parameter is set to 0 for IP Office environment. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ENABLE_SIP_USER_ID | 0 | Specifies the display of the user ID input field on the Login Screen.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled |
| ENABLE_SIPURI_HOST_VALIDATION | 1 | Specifies allowing to accept SIP URI with unrecognized host part in INVITE message.<br>Value operation:<br>• 0: Does not allow<br>• 1: Allows |
| 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.<br>Value operation:<br>• 0: No validation.<br>• 1: Validates the phone registration. |
| ENABLE_USBHEADSET | 1 | Specifies whether the USB headset feature is enabled or not.<br>Value operation:<br>• 0: Disabled<br>• 1: enabled |
| ENABLE_USBKEYBOARD | 1 | It enables or disables the USB keyboard support.<br>This parameter ignores the other values if the value is set to 1 (enabled by default).<br>Value operation:<br>0: Disabled<br>1: Enabled<br>**Note:**<br>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.<br>This parameter ignores the other values if the value is set to 1 (enabled by default).<br>Value operation:<br>0: Disabled<br>1: Enabled<br>**Note:**<br>This feature is available only on the Avaya J159 IP Phone and Avaya J189 IP Phone. |
| ENABLE_WEBSERVER | 1 | Enables or disables the web server to configure the phones in a web browser.<br>Value operation:<br>• 0: Disable<br>• 1: Enable |
| ENABLE_WMLPUSH_ALEDISPLAY_NAMERTING | 0 | Specifies the behavior of WML browser during incoming call.<br>Value operation:<br>0 (Default): WML browser disappears when the phone starts ringing and an incoming call appears instead.<br>1: WML browser still appears when the phone starts ringing and user can answer a call by off-hook from WML browser application.<br>**Note:**<br>This feature is available only on the Avaya J159 IP Phone, Avaya J169/J179 IP Phone, and Avaya J189 IP Phone |
| ENCRYPT_SRTCP | 0 | Specifies whether RTCP packets are encrypted or not. SRTCP is only used if SRTP is enabled using MEDIAENCRYTIONRTCP. ENCRYPT_SRTCP parameter controls RTCP encryption for RTCP packets exchanged between peers. RTCP packets sent to Voice Monitoring Tools are always sent unencrypted.<br>Value operation:<br>• 0: SRTCP is disabled.<br>• 1: SRTCP is enabled. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ENFORCE_SIPS_URI | 1 | Specifies if a SIPS URI must be used for SRTP.<br>Value operation:<br>• 0: Not enforced<br>• 1: Enforced |
| ENHDIALSTAT | 1 | Specifies if the algorithm defined by the parameter is used during certain dialing behaviors.<br>Value operation:<br>• 0: Disables algorithm.<br>• 1: Enables algorithm, but not for contacts.<br>• 2: Enables algorithm including contacts.<br>**Note:**<br>The parameter is set to 0 for IP Office environment. |
| ENTRYNAME | 0 | Specifies if the calling party name, or the VDN or the skill name must be used in **History** entries.<br>Value operation:<br>• 0: Calling Party Name is used.<br>• 1: VDN or the skill name is used.<br>**Note:**<br>Avaya J129 IP Phone does not support this parameter. |
| EVENT_NOTIFY_AVAYA_MAX_USERS | 20 | Specifies the maximum number of users to be included in an event notification message from CM/AST-II or Avaya Aura® Conferencing 6.0 or later.<br>Valid values are 0 through 1000.<br>This parameter is used only for development and debugging purposes. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| EXCHANGE_AUTH_USERNAME_FORMAT | 0 | Specifies the necessary format of the username for http authentication.<br>Value operation:<br>• 0: Office 2003/Office2016 username format. Username= <ExchangeUserDomain\ExchangeUserAccount> or Username= <ExchangeUserAccount> if <ExchangeUserDomain> is empty.<br>• 1: Office 365 format. Username= <ExchangeUserAccount@ExchangeUserDomain> or Username= <ExchangeUserAccount> if <ExchangeUserDomain> is empty.<br>**Note:**<br>Only Avaya J129 IP Phone supports this feature. |
| EXCHANGE_AUTH_METHOD_DEFAULT | 0 | Specifies the Exchange authentication method configured by administrator.<br>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.<br>When you configure non-forced method, phone user can change the authentication method from the phone user interface and configure the active authentication method.<br>Value operation:<br>• **0**: Basic authentication (Default)<br>• **1**: OAuth authentication<br>• **2**: Basic authentication- forced<br>• **3**: OAuth authentication- forced<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |
| EXCHANGE_EMAIL_DOMAIN | Null | Specifies the Exchange email domain.<br>The value can contain 0 to 255 characters.<br>**Note:**<br>Only Avaya J129 IP Phone supports this feature. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| EXCHANGE_NOTIFY_SUBSCRIPTION_PERIOD | 180 | Specifies the number of seconds between re-syncs with the Exchange server.<br>Valid values are 0 through 3600.<br>**Note:**<br>Avaya J159 IP Phone and Avaya J169/J179 IP Phone support this parameter. |
| EXCHANGE_REMINDER_TIME | 5 | Specifies the number of minutes before an appointment at which a reminder will be displayed.<br>Valid values are 0 through 60.<br>**Note:**<br>Avaya J159 IP Phone and Avaya J169/J179 IP Phone support this parameter. |
| EXCHANGE_REMINDER_TONE | 1 | Specifies whether or not a tone will be generated the first time an Exchange reminder is displayed.<br>Value operation:<br>• 0: Tone not generated.<br>• 1: Tone generated.<br>**Note:**<br>Avaya J159 IP Phone and Avaya J169/J179 IP Phone support this parameter. |
| EXCHANGE_SERVER_LIST | outlook.office365.com | Specifies a list of one or more Exchange server IP addresses.<br>Addresses can be in dotted-decimal or DNS name format, separated by commas without any intervening spaces.<br>The list can contain up to 255 characters. |
| EXCHANGE_SERVER_SECURE_MODE | 1 | Specifies if HTTPS should be used to contact Exchange servers.<br>Value operation:<br>• 0: Use HTTP<br>• 1: Use HTTPS<br>**Note:**<br>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.<br>Valid values are 0 through 60.<br>**Note:**<br>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.<br>If phone user hasn't configured any user name on the phone user interface then value configured in this parameter would be used.<br>The valid value is a string of up to 255 characters. The default value is empty.<br>**Note:**<br>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 parameter is used as a part of the user authentication.<br>The value can contain 0 to 255 characters. |
| F | | |
| 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** softkey.<br>Valid values are 5 through 999. |
| FAST_RESPONSE_TIMEOUT | 4 | Specifies the number of seconds the phone will wait before terminating an INVITE transaction if no response is received.<br>Valid values are 0 through 32.<br>Value of 0 means that this timer is disabled. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| FIPS_ENABLED | 0 | Specifies whether only FIPS-approved cryptographic algorithms will be supported.<br>Value operation:<br>• 0: No restriction on using non FIPS-approved cryptographic algorithms.<br>• 1: Use only FIPS-approved cryptographic algorithms using embedded FIPS 140-2-validated cryptographic module. |
| FORBIDDEN_SESSION_REMOVAL_TIMER | 10 | Specifies the duration of an off-hook session before a call automatically ends. This is valid when there are no call appearances available on the called or remote party.<br>Valid values are from 5 to 20 seconds. |
| FORCE_DOT1XID | $MACADDR | Specifies the username ID the phone provides to the 802.1x authentication server.<br>This parameter is valid when you configure DOT1XEAPS as MD5 or PEAP.<br>Valid value is a string ranging from 1-31 characters. A valid value overwrites any other configuration made through the Administration menu or the web interface.<br>The default value is $MACADDR, the Ethernet MAC address of the phone.<br>If the value contains $SERIALNO, it is replaced by the telephone serial number.<br>$SERIALNO_UPPER and $MACADDR_UPPER are replaced by the same values as $SERIALNO and $MACADDR but in upper case. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| FORCE_DOT1XID_TLS | $MACADDR | Specifies the Ethernet 802.1x identity.<br><br>This parameter is valid when you configure DOT1XEAPS as TLS.<br><br>Valid value is a string ranging from 1-31 characters. A valid value overwrites any other configuration made through the Administration menu or the web interface.<br><br>The default value is $MACADDR, the Ethernet MAC address of the phone.<br><br>If the value contains $SERIALNO, it is replaced by the telephone serial number.<br><br>$SERIALNO_UPPER and $MACADDR_UPPER are replaced by the same values as $SERIALNO and $MACADDR but in upper case.<br><br>**Note:**<br><br>Avaya J129 IP Phone does not support this feature. |
| FORCE_DOT1XPSWD | Null | Specifies the password the phone provides to the 802.1x authentication server.<br><br>This parameter is valid when you configure DOT1XEAPS as MD5 or PEAP.<br><br>Valid value is a string ranging from 1-31 characters. A valid value overwrites any other configuration made through the Administration menu or the web interface.<br><br>The default value is Null.<br><br>If the value contains $MACADDR, it is replaced by the Ethernet MAC address of the phone.<br><br>If the value contains $SERIALNO, it is replaced by the telephone serial number.<br><br>$SERIALNO_UPPER and $MACADDR_UPPER are replaced by the same values as $SERIALNO and$MACADDR but in upper case. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| FORCE_HTTP_AUTH_USERNAME | Null | Specifies the username for HTTP provisioning server authentication.<br>The valid value is a string of up to 255 ASCII characters without any intervening spaces.<br>Double quotes (“”) must not be used in a username string, when you configure this parameter through the `46xxsettings.txt` file.<br>The following symbols are not supported when provisioning the credentials with the DHCP Option 242:<br>• Double quote mark (“”)<br>• Apostrophe (’)<br>• Comma (,)<br>• Equal sign (=) |
| FORCE_HTTP_AUTH_PASSWORD | Null | Specifies the password for HTTP provisioning server authentication.<br>The valid value is a string of up to 255 ASCII characters without any intervening spaces.<br>Double quotes (“”) must not be used in password string, when you configure this parameter through the `46xxsettings.txt` file.<br>The following symbols are not supported when provisioning the credentials with the DHCP Option 242:<br>• Double quote mark (“”)<br>• Apostrophe (’)<br>• Comma (,)<br>• Equal sign (=) |
| FORCE_SIP_EXTENSION | Null | Replaces User ID entered by the user during login. |
| FORCE_SIP_PASSWORD | Null | Replaces password entered by the user during login. |
| FORCE_SIP_USERNAME | Null | Replaces the user field entered by the user during login. |
| FORCE_WEB_ADMIN_PASSWORD | Null | Specifies the password to access the phone through Web as Administrator.<br>Valid values are 8 to 31 alphanumeric characters. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| 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 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.<br><br>Valid values are 96 through 127. |
| GMTOFFSET | 0:00 | Specifies the time offset from GMT in hours and minutes.<br><br>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). |
| GROUP | 0 | Specifies specifically-designated groups of phones by using IF statements based on the GROUP parameter.<br><br>The value of GROUP can be set manually in a phone by using the GROUP local admin procedure.<br><br>The default value of GROUP in each phone is 0, and the maximum value is 999. |
| 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.<br><br>Valid values are integers from 1 to 12.<br><br>**Note:**<br><br>This parameter is supported by Avaya J159 IP Phone and Avaya J169/J179 IP Phone. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| GUESTLOGINSTAT | 0 | Specifies whether the Guest Login feature is available to users.<br>Value operation:<br>• 0: The feature is not available.<br>• 1: The feature is availble..<br>**Note:**<br>This parameter is supported by Avaya J159 IP Phone and Avaya J169/J179 IP Phone. |
| 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.<br>Valid values are integers from 1 to 15. |
| H | | |
| HANDSET_PROFILE_DEFAULT | 1 | Specifies the number of the default handset audio profile.<br>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.<br>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. |
| HEADSET_PROFILE_DEFAULT | 1 | Specifies the number of the default headset audio profile.<br>Valid values are 1 through 20.<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| HEADSET_PROFILE_NAMES | Null | Specifies an ordered list of names to be displayed for headset audio profile selection.<br>The list can contain 0 to 255 UTF-8 characters.<br>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.<br>**Note:**<br>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.<br>Value operation:<br>• 0: The phone goes on-hook if the disconnect message is received when the headset is active.<br>• 1: Disconnect messages are ignored when the headset is active. This is used for Call Center setting. |
| HOMEIDLETIME | 10 for Avaya J129 IP Phone<br>0 for other models | Specifies the number of minutes of idle time after which the **Home** screen is displayed.<br>Valid values are 0 through 30.<br>A value of 0 means that the **Home** screen is not displayed automatically when the phone is idle. |
| HOTLINE | Null | Specifies zero or one hotline number.<br>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.<br>The value can contain 0 to 255 characters. The default value is null. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| 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 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.<br>The value can contain 0 to 127 ASCII characters without space. |
| HTTPPORT | 80 | Sets the TCP port used for HTTP file downloads from non-Avaya servers.<br>Values range from 0 to 65535. |
| 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.<br>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.<br>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:<br>• Dotted decimal<br>• Colon-hex<br>• DNS name<br>The parameter can be set by using LLDP.<br>Valid values contains 0 to 255 ASCII characters. |
| I | | |
| ICMPDU | 1 | Specifies if ICMP Destination Unreachable messages are generated.<br>Value operation:<br>• 0: No messages are generated.<br>• 1: Limited port unreachable messages are generated.<br>• 2: Protocol and port unreachable messages are generated. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| ICMPRED | 0 | Specifies if received ICMP Redirect messages are processed.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| 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.<br>Value Operation:<br>• 0: A display name in the Contact header is permitted to be used (default).<br>• 1: A display name in the Contact header is always ignored. |
| 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.<br>Value operation:<br>• 0: No<br>• 1: Yes<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |
| INGRESS_DTMF_VOL_LEVEL | -12dBm | Specifies the power level of tone, expressed in dBm0.<br>Values can range from -20dBm to -7dBm. |
| INTER_DIGIT_TIMEOUT | 5 | Specifies the number of seconds that the phone waits after a digit is dialed before sending a SIP INVITE.<br>Valid values are 1 through 10. |
| IPV6DADXMITS | 1 | Specifies whether Duplicate Address Detection is performed on tentative addresses, as specified in RFC 4862.<br>Value operation:<br>• 0: DAD is disabled<br>• 1 to 5: Maximum number of transmitted Neighbor Solicitation messages. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| IPV6STAT | 1 | Specifies whether IPv6 will be supported or not.<br>Value operation:<br>• 0: IPv6 will not be supported.<br>• 1: Dual mode.<br>• 2: IPv6 only mode. |
| K | | |
| 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.<br>Value operation:<br>• 0: Key Usage checking is disabled<br>• 1: Key Usage checking is enabled |
| L | | |
| 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.<br>Valid values:<br>• 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.<br>• 1 - Enable (default). When a call on the selected line is ended, the highlighted line is not changed. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| L2Q | 0 | Specifies if layer 2 frames generated by the telephone have IEEE 802.1Q VLAN tags.<br>Value operation:<br>• 0: Auto. VLAN tagging is turned on when the network can support VLAN tagging and L2QVLAN is non zero.<br>• 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.<br>• 2: Off. VLAN functionality is disabled.<br>**Note:**<br>This parameter can also be set through:<br>• Local admin procedure<br>• A name equal to value pair in DHCPACK message<br>• SET command in a settings file<br>• DHCP option 43<br>• LLDP |
| L2QAUD | 6 | Specifies the layer 2 priority value for audio frames generated by the telephone.<br>Valid values are 0 through 7.<br>**Note:**<br>This parameter can also be set through:<br>• SET command in a settings file<br>• 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.<br>Valid values are 0 through 7.<br>**Note:**<br>This parameter can also be set through:<br>• SET command in a settings file<br>• LLDP<br>• AADS<br>Setting this parameter through LLDP or AADS overwrites values in the settings file. |
| L2QVID | 5 | Specifies the layer 2 priority value for video frames generated by the phone.<br>Valid values are 0 through 7. |
| L2QVLAN | 0 | Specifies the voice VLAN ID to be used by IP phones.<br>Valid values are 0 through 4094.<br>**Note:**<br>This parameter can also be set through:<br>• Local admin procedure<br>• A name equal to value pair in DHCPACK message<br>• SET command in a settings file<br>• DHCP option 43<br>• LLDP |
| LANGUAGES | Null | Specifies the language files that must be installed or downloaded to the phone.<br>Filenames can be full URL, relative pathname, or filename comma separated filenames ending with `.xml`. |
| LLDP_ENABLED | 2 | Specifies whether LLDP is enabled.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled<br>• 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.<br>Value operation:<br>• 0: User does not need to dial area code.<br>• 1: User need to dial area code. When enabled, the area code parameter (PHNLAC) should also be configured.<br>**Note:**<br>This parameter is supported when the phone is failed over. |
| LOCALLY_ENFORCE_PRIVACY_HEADER<br>The parameter is only available in an Avaya Aura® environment. | 0 | Specifies whether the phone displays Restricted instead of CallerId information when a Privacy header is received in a SIP INVITE message for an incoming call.<br>Value operation:<br>• 0: Disabled. CallerID information is displayed.<br>• 1: Enabled. Restricted is displayed. |
| LOG_CATEGORY | Null | Specifies a list of categories of events to be logged through syslog and locally.<br>This parameter must be specified to log events below the Error level.<br>The list can contain up to 255 characters.<br>Category names are separated by commas without any intervening spaces. |
| 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.<br>The FAC code is identified by * or # entered as a first character.<br>Value operation:<br>• 0: Allow dialed FAC code to be replaced with a remote party number in the call history<br>• 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 formatl (IPv4), colon-hex format (IPv6, if supported), or DNS name format.<br>The value can contain 0 to 255 characters. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| LOGSRVR_SECURE | 0 | Specifies if the phone uses secure or non-secure syslog transport mode by default.<br>Value operation:<br>• 0: Non-secure mode using UDP transport<br>• 1: Secure mode using TLS transport RFC 5425<br>Selected value is available as Default option in Administrator menu |
| M | | |
| MATCHTYPE | 0 | Specifies how an incoming or outgoing phone number is compared with the contacts on the phone to display the contact name.<br>0: Displays the contact name if all the digits match.<br>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.<br>2: Displays the contact name if atleast the last four digits match. If the contacts are saved in multiple sources, for example, PPM, Exchange, or locally, the contact name saved first is displayed. |
| MAX_TRUSTCERTS | 10 | Specifies the maximum number of trusted certificates files defined by this parameter that can be downloaded to the phone. MAX_TRUSTCERTS enforces the number of certificates. Valid values are from 1 to 10. |
| MEDIA_ADDR_MODE | 4 | Specifies the IP address of the endpoint when both IPv4 and IPv6 addresses are provided. This parameter is used for SIP signalling.<br>Value operation:<br>• 4: IPv4<br>• 6: IPv6<br>• 46: Prefer IPv4 over IPv6<br>• 64: Prefer IPv6 over IPv4 |
| 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.<br>Value operation:<br>• 0: Remote or offerer's preference<br>• 1: Local |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| MEDIA_PRESERVATION | 1 | Supports media preservation when ENABLE_IPOFFICE is set to 2.<br>Value operation:<br>• 0: Phone tries to preserve a call for a duration specified by PRESERVED_CALL_DURATION settings parameter.<br>• 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. |
| MEDIAENCRYPTION | 9 | Specifies which media encryption (SRTP) options are supported.<br>3 options can be specified in a comma-separated list.<br>The options must match those specified in Avaya Aura® Communication Manager IP-codec-set form.<br>• 1: aescm128-hmac80<br>• 2: aescm128-hmac32<br>• 3: aescm128-hmac80-unauth<br>• 4: aescm128-hmac32-unauth<br>• 5: aescm128-hmac80-unenc<br>• 6: aescm128-hmac32-unenc<br>• 7: aescm128-hmac80-unenc-unauth<br>• 8: aescm128-hmac32-unenc-unauth<br>• 9: none (default)<br>• 10: aescm256-hmac80<br>• 11: aescm256-hmac32<br>The list of media encryption options is ordered from high (left) to the 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.<br>Avaya Aura® Communication Manager (CM) has the capability to change the list order in the SDP-OFFER (for audio only) when it passes through CM.<br>Do not use unauthenticated media encryption (SRTP) files. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| MLPP_MAX_PREC_LEVEL | 1 | Specifies the maximum allowed precedence level for the user.<br>Value operation:<br>• 1: Routine<br>• 2: Priority<br>• 3: Immediate<br>• 4: Flash<br>• 5: Flash Override<br>**Note:**<br>Only Avaya J129 IP Phone supports this feature. |
| MLPP_NET_DOMAIN | Null | Specifies the MLPP network domain.<br>Value operation:<br>• Null: No domain configured<br>• DSN: DSN network.<br>• UC: UC network. |
| MP_ENABLED | 0 | Specifies if the Multicast Paging feature is enabled on the phone.<br>This is the basic parameter for this feature. If this parameter is not set, other parameters listed below will be ignored.<br>Valid values:<br>• 0: Multicast Paging is disabled.<br>• 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.<br><br>The paging groups should be separated with a comma (“,”), and should be listed in the following format:<br>`IP:port:priority:label`<br><br>where<br><br>• `IP` is the multicast IP address of an MP group;<br><br>• `Port` is the IP port of a Multicast Paging group, the valid value is an even integer ranging from 1024 to 65534;<br><br>• `Priority` is the priority of a group. Allowed values are 1 through 16, with smaller values indicating a higher priority;<br><br>• `Label` is a group label which is displayed in notification messages when the incoming page from this group is played.<br><br>All the above-listed settings are required.<br><br>For example,<br>`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.<br><br>The paging groups should be separated with a comma (“,”) and should be listed in the following format:<br>`IP:port:label`<br><br>`IP`, `Port`, and `Label` denote the same as the corresponding MP_GROUPS_TO_LISTEN values. All these settings are required.<br><br>For example,<br>`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.<br>Valid values:<br>• 1: G.729 codec is used.<br>• 2: G.711u codec is used.<br>• 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.<br>The value must be valid for the selected codec and therefore must not be changed unless necessary. |
| MSGNUM | Null | Specifies the phone number to be dialed automatically when the user presses the Message button. The phone number connects to the user's voice mail system.<br>**Note:**<br>This parameter is applicable in Avaya Aura environment. In case of IP Office and third party environment, use the parameter PSTN_VM_NUM. |
| MTU_SIZE | 1500 | Specifies the maximum transmission unit (MTU) size transmitted by the phone.<br>Valid values are 1496 or 1500. Use 1496 for older Ethernet switches. |
| MUTE_ON_REMOTE_OFF_HOOK | 0 | Controls the speakerphone muting for a remote-initiated (a shared control or OOD-REFER) speakerphone off-hook.<br>Value operation:<br>• 0: The speakerphone is unmuted.<br>• 1: The speakerphone is muted.<br>The value is applied to the phone only when the phone is deployed with a Avaya Aura® Communication Manager 6.2.2 and earlier releases. If the phone is deployed with Avaya Aura® Communication Manager 6.3 or later, the setting is ignored. Instead the feature is delivered through PPM. The Turn on mute for remote off-hook attempt parameter is enabled in the station form through the Avaya Aura® Session Manager or Avaya Aura® Communication Manager (SAT) administrative interfaces.<br>**Note:**<br>This parameter is set to 0 in IP Office environment. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| 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.<br>The value can contain zero to 255 ASCII characters.<br>The parameter is only available in an Avaya Aura® environment. |
| MYCERTCN | $SERIALNO | Specifies the Common Name (CN) used in the SUBJECT of an SCEP certificate request.<br>The value must be a string that contains either $SERIALNO (which is replaced by the phone serial number in upper case) or $MACADDR (which is replaced by the phone MAC address in lower case), but it can contain other characters as well, including spaces.<br>$MACADDR_UPPER is replaced by the same value as $MACADDR but in upper case.<br>In order to use enhanced certificate renewal in SMGR 8.1.3 and later, the value of MYCERTCN parameter must remain unchanged from the one used in existing identity certificate. Enhanced certificate renewal fails if this value is changed. If a new value is explicitly desired, then either remove the parameter SCEP_ENTITY_CLASS or remove the existing certificate by using DELETE_MY_CERT parameter and re-install a new one.<br>The value can contain eight ($MACADDR) to 255 characters. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| MYCERTDN | Null | Specifies the part the SUBJECT of an SCEP certificate request that is common for all phones.<br><br>The value must begin with a / and can include Organizational Unit, Organization, Location, State and Country.<br><br>In order to use enhanced certificate renewal in SMGR 8.1.3 and later, the value of MYCERTDN parameter must remain unchanged from the one used in existing identity certificate. Enhanced certificate renewal fails if this value is changed. If a new value is explicitly desired, then either remove the parameter SCEP_ENTITY_CLASS or remove the existing certificate by using DELETE_MY_CERT parameter and re-install a new one.<br><br>The value can contain Zero to 255 ASCII characters.<br><br>**Note:**<br><br>/ must 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.<br><br>The value is a 4 ASCII numeric digits. The phone supports only value 2048. |
| MYCERTRENEW | 90 | Specifies the percentage of the identity certificate's validity interval after which renewal procedure is initiated.<br><br>For example: if you set the MYCERTRENEW 90, certificate validity is 365 days, the renewal time is calculated as = (365)-(365*90%)= 36.5 days before the expiry.<br><br>Valid values are 1 through 99. |
| MYCERTURL | Null | Specifies the URL of the SCEP server for obtaining an identity certificate.<br><br>The URL can be HTTP or HTTPS.<br><br>The valid values can range from Zero to 255 ASCII characters. |
| N | | |
| 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.<br><br>Valid values are 1 through 60. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| O | | |
| OCSP_ACCEPT_UNK | 1 | Specifies whether in cases where certificate revocation status for a specific certificate cannot be determined to bypass certificate revocation operation for this certificate.<br>Value operation:<br>• 0: Certificate is considered to be revoked if the certificate revocation status is unknown. TLS connection will be closed.<br>• 1: Certificate revocation operation will accept certificates for which the certificate revocation status is unknown. |
| OCSP_CACHE_EXPIRY | 2880 | Specifies the time interval for the OCSP cache expiry in minutes. OCSP response cache expiry uses nextUpdate value in OCSP response message. If nextUpdate is not present, then OCSP_CACHE_EXPIRY parameter value is used.<br>Valid range is from 60 to 10080 |
| OCSP_ENABLED | 0 | Specifies that OCSP is used to check the revocation status of the certificates.<br>Value operation:<br>• 0: Disabled. Certificate revocation checking is not performed.<br>• 1: Enabled. Certificate revocation checking is performed. |
| OCSP_HASH_ALGORITHM | 0 | Specifies the hashing algorithm for OCSP request.<br>Value operation:<br>• 0: SHA1 hash algorithm<br>• 1: SHA256 hash algorithm |
| OCSP_NONCE | 1 | Specifies whether a nonce is added in OCSP requests and expected in OCSP responses.<br>Value operation:<br>• 0: Not added to OCSP request.<br>• 1: Added to OCSP request. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| OCSP_TRUSTCERTS | Null | Specifies a list of OCSP trusted certificates. These certificates are used as the signing authority to verify the revocation status of a digital certificate, when the OCSP responder has a different CA than the root CA of the certificate.<br>This parameter supports 0 to 255 ASCII characters. The file names or URLs must be comma separated values without intervening spaces. You can use a maximum of six certificates. |
| 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.<br>Value operation:<br>• 1: Use the OCSP_URI and then the OCSP field of the Authority Information Access (AIA) extension of the certificate.<br>• 2: Use 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.<br>Value operation:<br>• 0: OCSP is not used. Always check with OCSP responder.<br>• 1: OSCP cache caching is used. |
| OFF_HOOK_ALERT_TIMER | 10 | Specifies the length of the alert timer in seconds<br>Value operation:<br>• 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.<br>Value operation:<br>• "": Disabled<br>• An extension number: The phone dials this number in case of an off-hook alert event. |
| OPUS_PAYLOAD_TYPE | 116 | 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 range is between 96 to 127. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| OUTBOUND_SUBSCRIPTION_REQUEST_DURATION | 86400 | Specifies the duration in seconds requested by the phone in SUBSCRIBE messages, which can be decreased depending on the response from the server.<br>Valid values are 60 through 31536000 (one year). The default value is 86400 (one day). |
| OVERRIDE_SOFTKEY_IDLE | 0 | Specifies if the phone shows default softkeys for CA lines in an IDLE state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_ACTIVE | 0 | Specifies if the phone shows default softkeys for CA lines in an ACTIVE state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_INCOMING | 0 | Specifies if the phone shows default softkeys for CA lines in an INCOMING state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_INCOMING_VISUAL | 0 | Specifies if the phone shows default softkeys for CA lines in an INCOMING_VISUAL state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_HELD | 0 | Specifies if the phone shows default softkeys for CA lines in an HELD state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_OUTGOING | 0 | Specifies if the phone shows default softkeys for CA lines in an OUTGOING state.<br>Value operation:<br>• 0: No<br>• 1: Yes |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| OVERRIDE_SOFTKEY_ACTIVE_PAGETARGET | 0 | Specifies if the phone shows default softkeys for CA lines in an ACTIVE_PAGE state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_DIALING | 0 | Specifies if the phone shows default softkeys for CA lines in a Dialing state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_DIALTONE | 0 | Specifies if the phone shows default softkeys for CA lines in an Dialtone state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_CONFERENCE_DIALING | 0 | Specifies if the phone shows default softkeys for CA lines in an Conference Dialing state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_CONFERENCE_OUTGOING | 0 | Specifies if the phone shows default softkeys for CA lines in an Conference Outgoing state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_CONFERENCE_CONSULT | 0 | Specifies if the phone shows default softkeys for CA lines in an Conference Consult state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_CONFERENCE_ACTIVE | 0 | Specifies if the phone shows default softkeys for CA lines in an Conference Consult state.<br>Value operation:<br>• 0: No<br>• 1: Yes |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| OVERRIDE_SOFTKEY_TRANSFER_DIALING | 0 | Specifies if the phone shows default softkeys for CA lines in an Transfer Dialing state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_TRANSFER_OUTGOING | 0 | Specifies if the phone shows default softkeys for CA lines in an Transfer Outgoing state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| OVERRIDE_SOFTKEY_TRANSFER_CONSULT | 0 | Specifies if the phone shows default softkeys for CA lines in an Transfer Consult state.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| P | | |
| PHNCC | 1 | Specifies the country code for United States. The value is 1.<br>Valid values 1 through 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.<br>If your extension is 12345, and your dial plan length is 5.<br>The maximum extension length is 13. This value must match the extension length set on your call server.<br>Valid values are 3 through 13. |
| PHNEMERGNUM | Null | Specifies an emergency phone number to be dialed if the associated button is selected.<br>Valid values can contain up to 30 dialable characters (0 to 9, *, #). |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| PHNIC | 011 | Specifies the international access code.<br>For the United States, the value is 011.<br>Valid values are from 0 to 4 dialable characters (0-9,*,#). |
| 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.<br>**Note:**<br>This parameter is supported when the phone is failed over. |
| PHNLD | 1 | Specifies the long distance access code.<br>Valid values are 0 through 9 and empty string.<br>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.<br>Valid values are 5 through 15. |
| PHNMUTEALERT_BLOCK | 1 | Specifies if the **Mute Alert** feature is blocked or unblocked.<br>Value operation:<br>• 0: Unblocked<br>• 1: Blocked |
| PHNNUMOFSA | 3 | Specifies the number of session appearances the phone must support while operating in a non-Avaya environment.<br>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.<br>Valid values are 0 to 2 dialable characters (0-9, *, #). |
| PHONEKEY | Null | Specifies the list of pre-configured keys.<br>For the PHONEKEY syntax rules and values, refer to Pre-configuration of keys parameter on page 213 and PHONEKEY parameter values on page 510. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| PHONE_LOCK_IDLETIME | 0 | Specifies the interval of idle time, in minutes, after which the phone will automatically lock.<br>The phone will lock irrespective of the value of ENABLE_PHONE_LOCK. |
| 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.<br>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.<br>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.<br>The value can be only digits, ranging between 4–20 characters.<br>if you do not set any value here, the SIP password can be used for unlocking the phone. |
| PHY1STAT | 1 | Specifies the speed and duplex settings for the Ethernet line interface.<br>Value operation:<br>• 1: auto-negotiate<br>• 2: 10Mbps half-duplex<br>• 3: 10Mbps full-duplex<br>• 4: 100Mbps half-duplex<br>• 5: 100Mbps full-duplex<br>• 6: 1Gbps full-duplex, if supported by hardware, otherwise auto-negotiated |
| PHY2_AUTOMDIX_ENABLED | 1 | Specifies whether auto-MDIX is enabled on PHY2.<br>Value operation:<br>• 0: auto-MDIX is disabled.<br>• 1: auto-MDIX is enabled. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| PHY2PRIO | 0 | Specifies the layer 2 priority value to be used for frames received on the secondary Ethernet interface when VLAN separation is enabled. The parameter is not supported when VLANSEPMODE is 1.<br>Valid values are 0 through 7.<br>**Note:**<br>J129 does not support this parameter. |
| PHY2STAT | 1 | Specifies the speed and duplex settings for the secondary (PC) Ethernet interface.<br>Value operation:<br>• 0: disabled<br>• 1: auto-negotiate<br>• 2: 10Mbps half-duplex<br>• 3: 10Mbps full-duplex<br>• 4: 100Mbps half-duplex<br>• 5: 100Mbps full-duplex<br>• 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.<br>Value operation:<br>• 0: Strip tags. VLAN tags are stripped from Ethernet frames leaving the computer (PC) port of the phone.<br>• 1: Does not strip tags. VLAN tags are not stripped from Ethernet frames leaving the Computer (PC) port of the phone.<br>**Note:**<br>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.<br>Valid values are 0 through 4094.<br>**Note:**<br>The parameter is configured through the following:<br>• SET command in a settings file<br>• LLDP |
| PKCS12_PASSWD_RETRY, PKCS12_2_PASSWD_RETRY, PKCS12_3_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.<br>Value operation:<br>• 0: No retry<br>For certificate profile 2 and 3, use PKCS12_2_PASSWD_RETRY and PKCS12_3_PASSWD_RETRY. |
| PKCS12URL,<br>PKCS12_2_URL<br>, PKCS12_3_URL | 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.<br>Value operation:<br>• Null: (Default) Specifies that the PKCS#12 identity certificate download is disabled.<br>• 0 – 255 characters.<br>To specify the URL for certificate profile 2 and 3, use PKCS12_2_URL and PKCS12_3_URL. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| PKCS12_USAGE | All | Specifies the list of services for which the certificate assigned to the PKCS12#1 profile is applied.<br>Valid values:<br>• SIP<br>• Provisioning<br>• 8021x<br>• LDAP<br>• Ring Central<br>• PUSH<br>• PPM<br>• XSI<br>• Syslog<br>• All(Default)<br>In case the usage value is set to All, the certificate is configured for all enabled services.<br>You can set the value to All, and exclude the services using !. For example:<br>When value is set to All, !Provisioning, it will set the value to all configured service except Provisioning. |
| PKCS12_2_USAGE | All | Specifies the list of services for which the certificate assigned to the PKCS12#2 profile is applied.<br>Valid values:<br>• SIP<br>• Provisioning<br>• 8021x<br>• LDAP<br>• Ring Central<br>• PUSH<br>• PPM<br>• XSI<br>• Syslog<br>• All(Default)<br>In case the usage value is set to All, the certificate is configured for all enabled services. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| PKCS12_3_USAGE | All | Specifies the list of services for which the certificate assigned to the PKCS12#3 profile is applied.<br>Valid values:<br>• SIP<br>• Provisioning<br>• 8021x<br>• LDAP<br>• Ring Central<br>• PUSH<br>• PPM<br>• XSI<br>• Syslog<br>• All(Default)<br>In case the usage value is set to All, the certificate is configured for all enabled services. |
| 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.<br>Value operation:<br>• 0: Stop ringback tone as soon as SDP is received.<br>• 1: Continue ringback tone until RTP is received (default). |
| PRESENCE_ACL_CONFIRM | 0 | Specifies the handling of a Presence ACL update with pending watchers.<br>Value operation:<br>• 0: Auto confirm. Automatically send a PUBLISH to allow presence monitoring (default).<br>• 1: Ignore. Take no action<br>This parameter is not supported in IP Office environment as presence is not supported. |
| 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.<br>The time interval can be from 10 minutes to 120 minutes. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| PRIVACY_SLAAC_MODE | 1 | Specifies the preference for Privacy Extensions.<br>Value operation:<br>• 0: Disable Privacy Extensions.<br>• 1: Enable Privacy Extensions and prefer public addresses to temporary addresses.<br>• 2: Enable Privacy Extensions and prefer temporary addresses to public addresses. |
| PROCPSWD | 27238 | Specifies an access code to access the admin menu procedures.<br>Valid values contain 0 through 7 ASCII numeric digits. The default value is 27238 unless indicated otherwise below. A null value implies that an access code is not required for access.<br>**Note:**<br>• Setting this parameter through PPM is more secure because this file can usually be accessed and read by anyone on the network. Setting the value in this file is intended primarily for configurations with versions of phone or if server software that do not support setting this value from the server.<br>• For enhanced security, use ADMIN_PASSWORD instead of PROCPSWD. |
| PROCSTAT | 0 | Specifies an access code to access the admin menu procedures.<br>Value operation:<br>• 0: Local procedures can be used (default).<br>• 1: Local procedures cannot be used. |
| PROVIDE_CF_RINGTONE | 0 | Specifies if the call forward ringtone option is provided to the user.<br>Value operation:<br>• 0: The call forward ringtone option is not provided (default).<br>• 1: The call forward ringtone option is provided. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| PROVIDE_EXCHANGE_CALENDAR | 1 | Specifies if menu items for exchange calendar are displayed.<br>Value operation:<br>• 0: Not displayed<br>• 1: Displayed (default) |
| PROVIDE_EXCHANGE_CONTACTS | 1 | Specifies if menu items for exchange contacts are displayed.<br>Value operation:<br>• 0: Not displayed<br>• 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.<br>Value operation:<br>• 0: Default (500ms) with user option (default).<br>• 1: Short (250ms) with user option.<br>• 2: Long (1000ms) with user option.<br>• 3: Very Long (2000ms) with user option.<br>• 4: No Repeat with user option.<br>• 5: Default (500ms) without user option.<br>• 6: Short (250ms) without user option.<br>• 7: Long (1000ms) without user option.<br>• 8: Very Long (2000ms) without user option.<br>• 9: No Repeat without user option.<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |
| PROVIDE_LOGOUT | 1 | Specifies if user can log out from the phone.<br>Value operation:<br>• 0: No<br>• 1: Yes<br>**Note:**<br>This parameter is set to 0 in IP Office environment. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| PROVIDE_NETWORKINFO_SCREEN | 1 | Specifies if the **Network Information** menu is displayed on the phone.<br>Value operation:<br>• 0: No<br>• 1: Yes |
| PROVIDE_OPTIONS_SCREEN | 1 | Specifies if **Options & Settings** menu is displayed on phone.<br>Value operation:<br>• 0: No<br>• 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.<br>Value operation:<br>• 0: The user menus are not displayed<br>• 1: The user menus are displayed |
| 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.<br>**Note:**<br>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.<br>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.<br>Value operation:<br>• 0: all Push requests are rejected for this Push type.<br>• 1: only the Push requests with Barge mode are accepted for this Push type.<br>• 2: the Push requests with Barge or Normal mode are accepted for this Push type.<br>The Push types controlled by each digit (11111) are the following:<br>• \|\|\|\|+- The rightmost digit controls Top line Push requests.<br>• \|\|\|+-- The next digit to the left controls display (WML browser) Push requests.<br>• \|\|+--- The next digit to the left controls receive audio Push requests.<br>• \|+---- The next digit to the left controls transmit audio Push requests.<br>• +----- The next digit to the left controls phonexml Push requests.<br>**Note:**<br>The display Push request (the WML browser) is supported only by the Avaya J159 IP Phone, Avaya J169/J179 IP Phone, and Avaya J189 IP Phone. |
| PUSHPORT | 80 | Specifies the TCP port number to be used by the HTTP server in the phone for push.<br>Valid values are 80 through 65535. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| PUSH_MODE | 2 | Specifies the combination of secure and non-secure Push to be used.<br>The Push mode ranges from 0-2 and is of the following types:<br>• 0: only non-secure Push is enabled.<br>• 1: only Secure Push is enabled.<br>• 2: Both secure and non-secure Push is enabled.<br>**Note:**<br>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. |
| Q | | |
| QLEVEL_MIN | 1 | Specifies the minimum quality level for which a low local network quality indication will not be displayed.<br>Value operation:<br>• 1: Never display icon (default)<br>• 2: Packet loss is > 5% or round trip network delay is > 720ms or jitter compensation delay is > 160ms.<br>• 3: Packet loss is > 4% or round trip network delay is > 640ms or jitter compensation delay is > 140ms.<br>• 4: Packet loss is > 3% or round trip network delay is > 560ms or jitter compensation delay is > 120ms.<br>• 5: Packet loss is > 2% or round trip network delay is > 480ms or jitter compensation delay is > 100ms.<br>• 6: Packet loss is > 1% or round trip network delay is > 400ms or jitter compensation delay is > 80ms.<br>**Note:**<br>Avaya J129 IP Phone does not support this parameter. |
| R | | |
| RDS_INITIAL_RETRY_ATTEMPTS | 15 | Specifies the number of retries after which the phone abandons its attempt to contact the PPM server.<br>Valid values are 1 through 30. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| RDS_INITIAL_RETRY_TIME | 2 | 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.<br>Valid values are 2 through 60. |
| RDS_MAX_RETRY_TIME | 600 | Specifies the maximum delay interval in seconds after which the phone abandons its attempt to contact the PPM server.<br>Valid values are 2 through 3600. |
| RECORDINGTONE_INTERVAL | 15 | Specifies the number of seconds between call recording tones.<br>Valid values are 1 through 60. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| RECORDINGTONE_VOLUME | 0 | Specifies the volume of the call recording tone in 5dB steps.<br>Value operation:<br>• 0: The tone volume is equal to the transmit audio level (default).<br>• 1: The tone volume is 45dB below the transmit audio level.<br>• 2: The tone volume is 40dB below the transmit audio level.<br>• 3: The tone volume is 35dB below the transmit audio level.<br>• 4: The tone volume is 30dB below the transmit audio level.<br>• 5: The tone volume is 25dB below the transmit audio level.<br>• 6: The tone volume is 20dB below the transmit audio level.<br>• 7: The tone volume is 15dB below the transmit audio level.<br>• 8: The tone volume is 10dB below the transmit audio level.<br>• 9: The tone volume is 5dB below the transmit audio level.<br>• 10: The tone volume is equal to the transmit audio level.<br>**Note:**<br>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.<br>Valid values are 10 through 36000. |
| REDIRECT_TONE | 1 | Specifies the tone to play when a call goes to coverage.<br>Valid values are from 1 to 4. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| REGISTERWAIT | 900 | Specifies the number of seconds between re-registrations with the current server. Valid values are from 30 to 86400. |
| RESTART_FROM_LOGIN | 0 | Specifies if the phone displays the Restart soft key from the Login screen. When the user presses the Restart soft key, the phone prompts to confirm the restart. Upon user confirmation, the phone restarts.<br>The options are:<br>• 0: Disable<br>• 1: Enable<br>**Note:**<br>Avaya J129 IP Phone does not support the restart of the phone from the Login screen. |
| REUSETIME | 60 | Specifies the number of seconds that the DHCP is attempted:<br>• With a VLAN ID of zero. True when L2Q is set to 1.<br>• With untagged frames. True if L2Q is set to 0 or 2.<br>• Before reusing the IP address and the associated address information, that the phone had the last time it successfully registered with a call server.<br>While reusing an address, DHCP enters the extended rebinding state described above for DHCPSTD.<br>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. |
| 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.<br>The list can contain 0 to 1023 UTF-8 characters. The default value is null.<br>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.<br>Value operation:<br>• 0: Phone only tries to download ring tones with new display names.<br>• 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**.<br>Value operation:<br>• 0: North American ring tones are offered (default).<br>• 1: European ring tones are offered. |
| RTCP_XR | 0 | Specifies whether and how VoIP Metrics Report Block as defined in RTP Control Protocol Extended Report is sent.<br>Value operation:<br>• 0: No Extended Report (RTCP XR) is sent.<br>• 1: Extended Report (RTCP XR) is sent to voice monitoring servers if it is configured, and to the remote peer.<br>• 2: Extended Report (RTCP XR) is sent only to voice monitoring servers if its configured.<br>You can configure the voice monitoring server using the parameter RTCPMON.<br>When you set RTCP_XR to value 1 or 2, the voice RTCP XR report is sent to RTCPMON. |
| RTCPMON | Null | Specifies the IP or DNS address for the RTCP monitor (VMM server) in dotted-decimal format or DNS name format.<br>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. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| RTCPMONPORT | 5005 | Specifies the RTCP monitor port number.<br>You can set this parameter only if the environment is not an Avaya environment. The values can range from 0 through 65535. Default is 5005. |
| RTP_PORT_LOW | 2048 | Specifies the lower limit of the UDP port range to be used by RTP or RTCP and SRTP or SRTCP connections.<br>The values can range from 1024 through 65503. |
| RTP_PORT_RANGE | 40 | Specifies the range or number of UDP ports available for RTP or RTCP and SRTP or SRTCP connections.<br>This value is added to RTP_PORT_LOW to determine the upper limit of the UDP port range.<br>The values can range from 32 through 63487. |
| S | | |
| 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.<br>If the value contains $SERIALNO, $SERIALNO is replaced by the phone serial number in upper case. If the value contains $MACADDR, $MACADDR is replaced by the phone MAC address in lower case without the colon separators. $MACADDR_UPPER is replaced by the value in upper case.<br>In order to use enhanced certificate renewal in SMGR 8.1.3 and later, SCEPPASSWORD value cannot be empty nor it can be set to a variable such as $MACADDR or $SERIALNO.<br>If you want to renew or enrollment using standard SCEP protocol, parameter SCEP_ENTITY_CLASS must be removed. |
| SCEPENCALG | 0 | Specifies SCEP Encryption Algorithm.<br>Value operation:<br>• 0: DES<br>• 1: AES-256<br>**Note:**<br>Avaya J129 IP Phone supports this parameter. |
| SCEP_ENTITY_CLASS, | Null | Specifies to use the enhanced SCEP enrollment request. The value of entity-class is set in SMGR. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| SCEP_USAGE | All | Specifies the list of services for which the certificate assigned to the SCEP#1 profile is applied.<br>Valid values:<br>• SIP<br>• Provisioning<br>• 8021x<br>• LDAP<br>• Ring Central<br>• PUSH<br>• PPM<br>• XSI<br>• Syslog<br>• All(Default)<br>In case the usage value is set to All, the certificate is configured for all enabled services. |
| SCEP_2_USAGE | All | Specifies the list of services for which the certificate assigned to the SCEP#2 profile is applied.<br>Valid values:<br>• SIP<br>• Provisioning<br>• 8021x<br>• LDAP<br>• Ring Central<br>• PUSH<br>• PPM<br>• XSI<br>• Syslog<br>• All(Default)<br>In case the usage value is set to All, the certificate is configured for all enabled services. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| SCEP_3_USAGE | All | Specifies the list of services for which the certificate assigned to the SCEP#3 profile is applied.<br>Valid values:<br>• SIP<br>• Provisioning<br>• 8021x<br>• LDAP<br>• Ring Central<br>• PUSH<br>• PPM<br>• XSI<br>• Syslog<br>• All(Default)<br>In case the usage value is set to All, the certificate is configured for all enabled services. |
| SCREENSAVER_CLOCK_ENABLE | 1 | Specifies whether to present clock on the screensaver. User can override the configuration in the settings menu.<br>Value operation:<br>• 0: Clock is not presented on screensaver.<br>• 1: Clock is presented on screensaver. |
| SCREENSAVER_IMAGE | N/A | Specifies the screen saver images those can be loaded from the provisioning server.<br>Maximum five custom images can be uploaded onto the phone. Only .jpeg format files are supported until software version 4.0.11 and earlier. From software version 4.0.12 and later, only .jpg format files are supported. The maximum file size is 256KB.<br>Note that the image file name is case sensitive. |
| SCREENSAVER_IMAGE_DISPLAY | N/A | Allows the administrator to display the desired screen saver image. Note that If BACKGROUND_IMAGE_SELECTABLE is set to 1 then the end user may override this setting. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| SCREENSAVER_IMAGE_DISPLAY_JEM | 1 | Specifies the screen saver image to be displayed on the Avaya J100 Expansion Module.<br>The value is separated by commas without any intervening spaces.<br>To select one of the seven built-in default images, need to specify a value from 0 to 6.<br>• 0: To select default image 1.<br>• 1: To select default image 2.<br>• 2: To select default image 3.<br>• 3: To select default image 4.<br>• 4: To select default image 5.<br>• 5: To select default image 6.<br>• 6: To select default image 7.<br>**Note:**<br>Note: If the parameter is not set, then a Avaya J100 Expansion Module screen saver image must be set to default Avaya device image. |
| SCREENSAVER_IMAGE_JEM | Null | Specifies a comma-separated list of screen saver images for the Avaya J100 Expansion Module display.<br>Avaya J100 Expansion Module supports up to 5 screen saver images with the following limitation:<br>• Only jpg format files are supported.<br>• The maximum file size is 256 KB.<br>• The file names are case sensitive.<br>• The color depth is limited to 16 bits.<br>The Avaya J100 Expansion Module has a resolution of 272 x 480 pixels.<br>The files must be stored in the directory specified by HTTPDIR or TLSDIR. |
| SCREENSAVER_IMAGE_JEM_FOLLOW_PRIMARY | 1 | Specifies whether the Avaya J100 Expansion Module screen saver image always follows the primary display or can have a separate screen saver image.<br>The options are:<br>• 0: You can configure a separate screen saver image for the Avaya J100 Expansion Module screen saver.<br>• 1: Avaya J100 Expansion Module screen saver image always follows the primary display. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| SCREENSAVER_IMAGE_SELECTABLE | 1 | Allows the end user to select and change the screen saver images.<br>Value operation:<br>• 0: End user can not select and change the screen saver images from the settings menu.<br>• 1: End user can select and change the screen saver images from the settings menu. |
| SCREENSAVER_IMAGE_SELECTABLE_JEM | Null | Specifies whether the user can select a screen saver image.<br>The options are:<br>• 0: The end user is not allowed to choose the Avaya J100 Expansion Module screen saver image. The value set by an administrator is used.<br>• 1: The end user is allowed to choose the Avaya J100 Expansion Module screen saver image. |
| SCREENSAVER_IMAGE_SECONDARY | Null | Specifies a list of screen saver images to be used on the secondary screen.<br>Maximum five custom images can be uploaded onto the phone. Only .jpeg format files are supported until software version 4.0.11 and earlier. From software release 4.0.12 and later, only jpg format files are supported. The maximum file size is 256KB.<br>Note that the image file name is case sensitive.<br>Example: screen saver_example1.jpg, screensaver_example2.jpeg<br>**Note:**<br>Avaya J159 IP Phone and Avaya J189 IP Phone supports this parameter. |
| 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.<br>Note that if SCREENSAVER_IMAGE_SELECTABLE_SECONDARY is set to 1 then the end user may override this setting.<br>Example: screensaver_example1.jpg<br>**Note:**<br>Avaya J159 IP Phone and Avaya J189 IP Phone supports this parameter. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| SCREENSAVER_IMAGE_SELECTABLE_SECONDARY | 1 | Allows the end user to select screen saver images for the secondary screen.<br>Value operation:<br>• 0: The user can not use a screen saver images from the phone UI.<br>• 1: The user can select a background images from the phone UI.<br>This parameter overrides the value configured using SCREENSAVER_IMAGE_DISPLAY_SECONDARY parameter.<br>**Note:**<br>Avaya J159 IP Phone and Avaya J189 IP Phone supports this parameter. |
| SCREENSAVERON | 240 (4 hours) | Specifies the number of minutes of idle time after which the screen saver is displayed.<br>If an image file is downloaded based on the LOGOS and CURRENT_LOGO parameter, it is used as the screen saver. Otherwise, the built-in Avaya one-X(TM) screen saver is used.<br>Valid values are 0 through 999. The default value is 240 (4 hours).<br>A value of 0 means that the screen saver will not be displayed automatically when the phone is idle. |
| SCROLLING_MODE | 0 | Specifies the scrolling mode used on the phone.<br>Value operation:<br>• `0`: Line scrolling mode is used.<br>• `1`: Page scrolling mode is used. |
| SDPCAPNEG | 1 | Specifies if SDP capability negotiation is enabled.<br>Value operation:<br>• 0: SDP capability negotiation is disabled.<br>• 1: SDP capability negotiation is enabled. |
| SEND_DTMF_TYPE | 2 | Specifies if DTMF tones are sent in-band as regular audio, or out-of-band using RFC 2833 procedures.<br>Value operation:<br>• 1: In-band<br>• 2: Out-of-band |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| SERVER_CERT_RECHECK_HOURS | 24 | Specifies the number of hours after which certificate expiration and OCSP will be used, if OCSP is enabled, to recheck the revocation and expiration status of the certificates that were used to establish a TLS connection. Valid values are from 0 to 32767.<br>Value operation:<br>• 0: Periodic checking is disabled. |
| SHORTCUT_ACTION_CONTACT, SHORTCUT_ACTION_AUTODIAL | 0 | Specifies the action performed if the user presses an Autodial key or selects a contact on the Phone screen during an active call.<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |
| SHOW_LAST_EXTENSION | 0 | Specifies whether to display last extension after logout.<br>Value operation:<br>• 0: To hide last extension after logout.<br>• 1: To display the last extension after logout. |
| 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.<br>Value operation:<br>0: Download the upgrade file for the same signaling protocol that is supported by the current software (default)<br>1: Download 96x1Hupgrade.txt (for H.323 software)<br>2: Download 96x1Supgrade.txt (for SIP software) |
| SIG_PORT_LOW | 1024 | Specifies the minimum port value for SIP signaling. (1024 -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 (32-64511). |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| 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.<br><br>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.<br><br>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.<br><br>Value operation:<br><br>• 4: IPv4<br><br>• 6: IPv6 |
| SIMULTANEOUS_REGISTRATIONS | 3 | Specifies the number of Session Managers with which the phone simultaneously register.<br><br>Valid values are 1, 2, 3, 4 or 5. The default value is 3.<br><br>**Note:**<br><br>This parameter is set to 1 in IP Office environment. |
| 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<br><br>• `host` is an proxy address in dotted-decimal or DNS name format.<br><br>• `[:port]` is an optional port number.<br><br>• `[;transport=xxx]` is an optional transport type where `xxx` can be TLS, TCP, or UDP.<br><br>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 contains the list of SIP Proxy or Registrar servers separated by comma when the SIP device is configured for the dual-stack operation.<br>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.<br>Valid values are 0 to 255 characters in the dotted decimal or colon-hex format.<br>The SIP Proxy list has the following format: `host[:port][;transport=xxx]` where<br>• `host` is IP addresses in dotted-decimal format or hex format.<br>• `[:port]` is the port number. The default values are 5060 for TCP and 5061 for TLS.<br>• `[;transport=xxx]` is the transport type and `xxx` is either TLS or TCP. The default value is TLS.<br>For example, `SIP_CONTROLLER_LIST_2="10.16.26.88:5060;transport=tcp"` |
| SIPDOMAIN | Null | Specifies the domain name to be used during SIP registration.<br>The value can contain 0 to 255 characters. The default value is null. |
| SIPPORT | 5060 | Specifies the port the phone opens to receive SIP signaling messages.<br>Valid values are 1024 through 65535. The default value is 5060. |
| SIPREGPROXYPOLICY | Simultaneous | Specifies if the phone attempts to maintain one or multiple simultaneous registrations.<br>Value operation:<br>• Alternate: Only a single registration is attempted and maintained.<br>• Simultaneous: Simultaneous registrations is attempted and maintained with all available controllers.<br>**Note:**<br>This parameter is supported only in IP Office environment. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| SKILLSCREENTIME | 5 | Specifies the duration, in seconds, that the **Skills** screen is displayed.<br>Valid values are 0 through 60. The default value is 5.<br>A value of 0 means that the **Skills** screen in not removed automatically when the agent logs in.<br>**Note:**<br>Avaya J129 IP Phone and Avaya J139 IP Phone do not support this feature. |
| SLMCAP | 0 | Specifies if the SLA Monitor agent is enabled for packet capture.<br>Value operation:<br>• 0: Disabled (default)<br>• 1: Enabled and payloads are removed from RTP packets<br>• 2: Enabled and payloads are included in RTP packets<br>• 3: Controlled from admin menu - Allows you to enable or disable of RTP packets capture using local admin procedures. |
| SLMCTRL | 0 | Specifies whether the SLA Monitor agent is enabled for phone control.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled<br>• 2: Controlled from admin menu. |
| SLMPERF | 0 | Specifies whether the SLA Monitor agent is enabled for phone performance monitoring.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| SLMPORT | 50011 | Specifies the UDP port that will be opened by the SLA Monitor agent to receive discovery and test request messages.<br><br>Valid values are 6000 through 65535. The default value is 50011.<br><br>**Note:**<br><br>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. |
| SLMSRVR | Null | Specifies the IP address and the port number of the SLA Mon server in the aaa.bbb.ccc.ddd:n format.<br><br>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.<br><br>Specifying a port number is optional. If you do not specify a port number, the system takes 50011 as the default port. If the value of the port number is 0, than any port number is acceptable.<br><br>The IP address must be in the dotted decimal format, optionally followed by a colon and an integer port number from 0 to 65535.<br><br>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 addressof the SLA Mon server.<br><br>**Note:**<br><br>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.<br><br>Value operation:<br><br>• 0: Disabled<br><br>• 1: Enabled inside an enterprise<br><br>• 2: Enabled for remote worker deployments |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| SMGR_AUTO_FAVORITE | 0 | Specifies whether all the Avaya Aura System Manager (SMGR) configured features and supported Autodials irrespective of adding it to favorite or not, are available on the phone screen. Use Avaya Aura 8.0.0.0 or earlier.<br>Value operation:<br>• 0: Do not auto-favorite<br>• 1: Auto-favorite<br>**Note:**<br>The phone does not support the display of Autodials without a number.<br>Avaya J129 IP Phone does not support this feature. |
| SNMPADD | Null | Specifies a list of source IP addresses from which SNMP query messages will be accepted and processed.<br>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.<br>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.<br>Valid values contain 0 through 32 ASCII alphanumeric characters.<br>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 2880 minutes. |
| SNTPSRVR | Null | Specifies a list of addresses of SNTP servers.<br>Addresses can be in dotted-decimal or DNS name format, separated by commas without any intervening spaces.<br>The list can contain up to 255 characters. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| SOFTKEY_ACTIVE_PAGETARGET | | 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.<br>For example:<br>`SET SOFTKEY_ACTIVE_PAGETARGET "type=dtmf;action=AnswerDigitSequence;label=Answer"`<br>`ADD SOFTKEY_ACTIVE_PAGETARGET "type=function;action=endcall;label=End"` |
| 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.<br>For example:<br>`SET SOFTKEY_ACTIVE "type=dtmf;action=##*3;label=Park"`<br>`ADD SOFTKEY_ACTIVE "type=dtmf;action=*34;label=Record"` |
| SOFTKEY_HELD | Null | Specifies the custom soft key for the call appearance lines in an Held state. You can provide the soft key attributes and labels, which a phone displays during an outgoing call, along with standard soft keys.<br>For example:<br>`SET SOFTKEY_HELD "type=function;action=endcall;label=drop"`<br>`ADD SOFTKEY_HELD "type=function;action=endcall;label=finish"` |
| SOFTKEY_CONFIGURATION | 0,1,2 | Specifies which feature will show up on which softkey on the Avaya J129 IP Phone screens.<br>The features are defined as follows:<br>• 0 = Redial<br>• 1 = Contacts<br>• 2 = Emergency<br>• 3 = Recents<br>• 4 = Voicemail |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| 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.<br>For example:<br>`SET SOFTKEY_IDLE "type=function;action=newcall;label=call"`<br>`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.<br>For example:<br>`SET SOFTKEY_INCOMING "type=function;action=newcall;label=call"`<br>`ADD SOFTKEY_INCOMING "type=function;action=decline;label=reject"` |
| 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.<br>For example:<br>`SET SOFTKEY_INCOMING_VISUAL "type=function;action=newcall;label=call"`<br>`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.<br>For example:<br>`SET SOFTKEY_OUTGOING "type=function;action=endcall;label=drop"`<br>`ADD SOFTKEY_OUTGOING "type=function;action=endcall;label=finish"` |

*Table continues…*

| Parameter name | Default value | 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.<br>For example:<br>`SET SOFTKEY_DIALING "type=function;action=redial;label=dial"`<br>`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.<br>For example:<br>`SET SOFTKEY_DIALTONE "type=function;action=redial;label=dial"`<br>`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.<br>For example:<br>`SET SOFTKEY_CONFERENCE_DIALING "type=function;action=clear;label=drop"`<br>`ADD SOFTKEY_CONFERENCE_DIALING "type=function;action=endcall;label=finish"` |
| 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.<br>For example:<br>`SET SOFTKEY_CONFERENCE_OUTGOING "type=function;action=cancel;label=drop"`<br>`ADD SOFTKEY_CONFERENCE_OUTGOING "type=function;action=clear;label=finish"` |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| 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.<br>For example:<br>`SET SOFTKEY_CONFERENCE_CONSULT "type=function;action=cancel;label=drop"`<br>`ADD SOFTKEY_CONFERENCE_CONSULT "type=function;action=endcall;label=finish"` |
| 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.<br>For example:<br>`SET SOFTKEY_CONFERENCE_ACTIVE "type=function;action=cancel;label=drop"`<br>`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.<br>For example:<br>`SET SOFTKEY_TRANSFER_DIALING "type=function;action=clear;label=drop"`<br>`ADD SOFTKEY_TRANSFER_DIALING "type=function;action=endcall;label=finish"` |
| 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.<br>For example:<br>`SET SOFTKEY_TRANSFER_OUTGOING "type=function;action=cancel;label=drop"`<br>`ADD SOFTKEY_TRANSFER_OUTGOING "type=function;action=clear;label=finish"` |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| 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.<br>For example:<br>`SET SOFTKEY_TRANSFER_CONSULT "type=function;action=cancel;label=drop"`<br>`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.<br>The options are:<br>• 0: Disabled, all Avaya Spaces features via APIs are disabled.<br>• 1: Guest only, Avaya Spaces feature can be accessed by guest/anonymous authentication only.<br>Connections to Avaya Spaces uses the embedded public certificates and any certificates defined in the TRUSTCERTS. It ignores ENABLE_PUBLIC_CA_CERTS.<br>**Note:**<br>This parameter is not supported on Avaya J129 IP Phone. |
| 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 Spacesdirect number then this defined direct number is used.<br>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 (+).<br>**Note:**<br>This parameter is not supported on Avaya J129 IP Phone. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| SPACES_DIRECT_NUMBER_PROVIDE | 1 | Specifies if the end user is allowed to select a direct number for a voice call to Avaya Spaces.<br>The options are:<br>• 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.<br>• 1: Show, user is allowed to select a direct number for a voice call to Avaya Spaces.<br>**Note:**<br>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.<br>This parameter is not supported on Avaya J129 IP Phone. |
| SPEAKERSTAT | 2 | Specifies the operation of the speakerphone.<br>Value operation:<br>• 0: Speakerphone disabled.<br>• 1: One-way speaker (also called monitor) enabled.<br>• 2: Full (two-way) speakerphone enabled.<br>**Note:**<br>This parameter is not supported on Avaya J129 IP Phone. |
| SSH_ALLOWED | 2 | Specifies if SSH is supported.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled<br>• 2: Configured using local admin procedure. When this mode is configured, then by default the SSH server is disabled. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| SSH_BANNER_FILE | Null | Specifies the file name or URL for a custom SSH banner file.<br>If the value is null, english banner is used for SSH.<br>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.<br>Valid values are 0 through 32767.<br>A value of 0 means that the connection will not be terminated. |
| SUBSCRIBE_LIST_NON_AVAYA | Null | Specifies comma separated list of event packages to subscribe to after registration.<br>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.<br>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.<br>Value operation:<br>• 0: The phone uses SIP for both the request URI and the contactheader regardless of whether SRTP is enabled.<br>• 1: The phone uses SIPS for both the request URI and the contact header if SRTP is enabled. TLS is on and MEDIAENCRYPTION has at least one valid crypto suite.<br>• 2: SES or PPM does not show a FS-phoneData FeatureName with a Feature Version of 2 in the response to the getHomeCapabilities request.<br>For IP office environment, the applicable values are 0 and 1. |

*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).<br>The list can contain up to 255 characters. Values are separated by commas without any intervening spaces.<br>If the value is set to null, subscribe messages are not sent. |
| SYMMETRIC_RTP | 1 | Specifies if the phone must discard received RTP or SRTP datagrams if their UDP source port number is not the same as the UDP destination port number included in the RTP or SRTP datagrams of that endpoint.<br>Value operation:<br>• 0: Ignore the UDP source port number in received RTP/SRTP datagrams.<br>• 1: Discard received RTP/SRTP datagrams if their UDP Source Port number does not match the UDP Destination Port number that the phone includes in RTP/SRTP datagrams intended for that phone. |
| SYSLOG_ENABLED | 0 | Specifies if sending Syslog messages is enabled or not.<br>Value operation:<br>• 0: Sending Syslog messages is disabled.<br>• 1: Sending Syslog messages is enabled.<br>**Note:**<br>The phone does not display the Secure call icon, if you set the parameter value to 1. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| SYSLOG_LEVEL | 4 | Specifies the severity level of syslog messages.<br>Events with the selected severity level and above will be logged. The lower numeric severity values correspond to higher severity levels.<br>Value operation:<br>• 3: Error, Critical, Alert and Emergency events are logged.<br>• 4: Warning, Error, Critical, Alert and Emergency events are logged (Default).<br>• 5: Notice, Warning, Error, Critical, Alert and Emergency events are logged.<br>• 6: Informational, Notice, Warning, Error, Critical, Alert and Emergency events are logged.<br>• 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.<br>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.<br>Valid values range from 0 through 32 ASCII characters.<br>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.<br>Valid values are from 5 through 60. |
| TCP_KEEP_ALIVE_STATUS | 1 | Specifies if the phone sends TCP keep alive messages.<br>Value operation:<br>• 0: Keep-alive messages are not sent.<br>• 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.<br>Valid values are from 10 through 3600 |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| 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.<br>Value operation:<br>• 0: Disabled. The redirect indication is shown only on a monitoring station which is redirection destination.<br>• 1: Enabled. The redirection indication is displayed on all monitoring stations.<br>**Note:**<br>Avaya J129 IP Phone and Avaya J139 IP Phone do not support this feature. |
| TEAM_BUTTON_RING_TYPE | 1 | Specifies the alerting pattern to use for team buttons.<br>Valid values are 1 through 8. The default value is 1.<br>**Note:**<br>Avaya J129 IP Phone and Avaya J139 IP Phone do not support Team Button feature. |
| TIMEFORMAT | 0 | Specifies the format for time displayed in the phone.<br>The TIMEFORMAT parameter is value is applied from the `46xxsettings.txt` file on the very first installation, and after resetting parameters to defaults and when 3rd party servers don't backup the settings.<br>Value operation:<br>• 0: AM or PM format.<br>• 1: 24 hour format. |
| TLS_VERSION | 0 | Specifies the TLS version used for all TLS connections (except SLA monitor agent).<br>Value operation:<br>• 0: TLS version 1.0 and 1.2 are supported.<br>• 1: TLS version 1.2 only is supported.<br>• 2: TLS version 1.3 only is supported. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| 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.<br>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.<br>Valid values are from 0 to 65535. |
| 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. |
| TLSSRVRID | 1 | Specifies how a phone evaluates a certificate trust.<br>Value operation:<br>• 0: Identity matching is not performed.<br>• 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.<br>A URI received in a push request is only used to obtain push content, if it matches one of these values.<br>The list can contain up to 255 characters.<br>Values are separated by commas without any intervening spaces.<br>If the value of TPSLIST is null, push is disabled. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| 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.<br>The list can contain up to 255 characters. ## Values are separated by commas without intervening spaces. |
| U | | |
| UPDATE_DIALED_NUMBER_ON_ANSWER | 0 | Specifies whether displayed dialed number is updated or not based the number provided in 200 OK after an answer.<br>Value operation:<br>• 0: Displayed dialed number is not updated based on 200 OK received after answer (default).<br>• 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.<br>Value operation:<br>• 0: Turn off USB power regardless of power source.<br>• 1: Turn on USB power only if Aux powered.<br>• 2: Turn on USB power regardless of power source.<br>• 3: Turn on USB power if Aux powered or PoE Class 3 power.<br>**Note:**<br>This parameter is supported only in Avaya J159 IP Phone and Avaya J189 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.<br>Value operation:<br>• 0: Use CONTACT URI of the transfer target in Refer-To header of REFER SIP request.<br>• 1: Use TO URI of the transfer target in Refer-To header of REFER SIP request. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| USE_EXCHANGE_CALENDAR | 0 | Specifies whether the Calendar synchronizes with the Microsoft Exchange.<br>Value operation:<br>• 0: To disable synchronization.<br>• 1: To enable synchronization.<br>**Note:**<br>Avaya J169/J179 IP Phone supports this parameter. |
| USER_STORE_URI | Nulll | Specifies the URI path of IP Office for storing user data.<br>**Note:**<br>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.<br>Valid values are 5 through 60.<br>**Note:**<br>Avaya J129 IP Phone and Avaya J139 IP Phone do not support this feature. |
| V | | |
| VLANSEPMODE | 0<br>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.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled<br>**Note:**<br>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.<br>Valid values are 0 through 999.<br>A value of zero means that DHCP tries with a non-zero VLAN ID forever.<br>**Note:**<br>This parameter is configured through:<br>• The settings file<br>• A name equal to value pair in DHCPACK message |
| VOLUME_UPDATE_DELAY | 2 | Specifies the minimum interval, in seconds, between backups of the volume levels to PPM service when the phone is registered to Avaya Aura® Session Manager.<br>If there is no change to volume levels, there will be no backup to PPM service.<br>Valid values are 2 through 900. The default value is 2. |
| 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.<br>Example: 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.<br>Valid values range from 0 to 4.<br>• 0: the notification is disabled<br>• 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.<br>Valid values are 30 through 180. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| WAIT_FOR_REGISTRATION_TIMER | 32 | Specifies the number of seconds that the phone waits for a response to a REGISTER request.<br>If no response message is received within this time, registration will be retried based on the value of RECOVERYREGISTERWAIT.<br>Valid values are 4 through 3600. |
| WAIT_FOR_UNREGISTRATION_TIMER | 32 | Specifies the number of seconds the phone waits before assuming that an un-registration request is complete.<br>Un-registration includes termination of registration and all active dialogs.<br>Valid values are 4 through 3600. |
| 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.<br>The value can contain 0 to 255 characters. |
| WBCSTAT | 1 | Specifies whether a wideband codec indication is displayed when a wideband codec is used.<br>Value operation:<br>• 0: Disabled<br>• 1: Enabled<br>**Note:**<br>Avaya J129 IP Phone does not support this feature. |
| WEB_ADMIN_PASSWORD | 27238 | Specifies the password to access the phone through a web browser as an administrator.<br>The value set from the web server interface has a higher priority than that of the settings file.<br>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.<br>Valid values are from 8 to 31 alphanumeric characters including upper, lower and special characters. |

*Table continues…*

| Parameter name | Default value | Description |
|---|---|---|
| WEB_HTTP_PORT | 80 | Specifies the port on which the Web Server running on the phone will be accessed using HTTP.<br>Valid values are 0, 80, 1024 to 65535. |
| WEB_HTTPS_PORT | 443 | Specifies the port on which the Web Server running on the phone will be accessed using HTTPS.<br>Valid values are 443, 1024 to 65535. |
| WEBSERVER_ON_HTTP | 0 | Specifies whether HTTP access to the web server is enabled or disabled.<br>To access WEB Server using HTTP set ENABLE_WEBSERVER and WEBSERVER_ON_HTTP to 1.<br>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.<br>Value operation:<br>• 0: Web Server is not accessible through HTTP.<br>• 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.<br>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.<br>The values are separated by commas without any intervening spaces.<br>The value can contain up to 255 characters.<br>Only Avaya J159 IP Phone, Avaya J169/J179 IP Phone, and Avaya J189 IP Phone 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** softkey is selected in the browser.<br>The allowed value contains not more than one URL of up to 255 characters.<br>Only Avaya J159 IP Phone, Avaya J169/J179 IP Phone, and Avaya J189 IP Phone support this parameter.<br>**Note:**<br>If the value is set to default, the WML browser is disabled. |
| WMLIDLETIME | 10 | Specifies the idle time in minutes after which the web page set as the value of WMLIDLEURI will be displayed.<br>The allowed value is a positive integer from 1 to 999.<br>Only Avaya J159 IP Phone, Avaya J169/J179 IP Phone, and Avaya J189 IP Phone support this parameter.<br>**Note:**<br>If WMLIDLEURI is set to null, the web page will not be displayed when the phone is idle. |
| 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.<br>The allowed value contains not more than one URL of up to 255 characters.<br>Only Avaya J159 IP Phone, Avaya J169/J179 IP Phone, and Avaya J189 IP Phone support this parameter. |
| WMLPORT | 8080 | Specifies the TCP port number of the HTTP proxy server set as the WMLPROXY value.<br>Allowed values are from 0 to 65535.<br>Only Avaya J159 IP Phone, Avaya J169/J179 IP Phone, and Avaya J189 IP Phone support this parameter. |
| WMLPROXY | Null | Specifies the IP addresses or domains for which the HTTP proxy server set as the WMLPROXY value will not be used.<br>Allowed values can contain up to 255 characters and must be separated by commas without any intervening spaces.<br>Only Avaya J159 IP Phone, Avaya J169/J179 IP Phone, and Avaya J189 IP Phone support this parameter. |

# List of Wi-Fi configuration parameters

| Parameter Name | Default Value | Description |
|---|---|---|
| WIFISTAT | `1` | Specifies the network interface to be used for network connectivity.<br>Value operation:<br>• `0`: Phone connects to only Ethernet network.<br>• `1`: Phone connects to Ethernet network, unless manually switched to Wi-Fi<br>• `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.<br>Value operation:<br>• `0`: Disabled<br>• `1`: Enabled |
| WLAN_ESSID | N/A | Specifies the wireless network to be used.<br>The name of the SSID ranges up to 32 characters. |
| WLAN_SECURITY | none | Specifies the security standard to be used for the wireless network.<br>Value operation:<br>• none: No security standard is defined.<br>• `wep`: WEP security standard is defined.<br>• `wpa2psk`: WPA2 security standard with pre-shared key is defined.<br>• `wpapsk`: WPA security standard with pre-shared key is defined.<br>• `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.<br>Value operation:<br>• 1<br>• 2<br>• 3<br>• 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.<br>Value operation:<br>• 0: Disable<br>• 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.<br>The valid values range from 0 to 4. |
| WEP_KEY_LEN | 128 bit | Specifies the length of the WEP key.<br>Value operation:<br>• 40 bit<br>• 64 bit<br>• 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`.<br><br>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.<br><br>Value operation:<br><br>• none- No phase 2 authentication (Default, but not currently supported)<br><br>• MSCHAPV2 : set to this value for forward compatibility<br><br>**Note:**<br><br>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.<br><br>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.<br><br>**Note:**<br><br>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.<br><br>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`.<br><br>Value operation:<br><br>• `PEAP`<br><br>• `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`.<br>The name must be from one to 32 characters.<br>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`.<br>The name must be from one to 32 characters.<br>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.<br>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.<br>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.<br>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.<br>Valid value is from 0 to 63. |

# 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** | `Type=DTMF` | Allows:<br>• 0 to 9<br>• Letters (a to z)<br>• Asterisk (*)<br>• Pound (#) | String value. Allows any UNICODE symbol, except for the following:<br>• Semicolon (;)<br>• Comma (,)<br>• Quote (“)<br>• Equal (=)<br>• Pipe (\|)<br>• Lesser than (<)<br>• Greater than (>)<br>• Forward slash (/)<br>• Ampersand (&) | |
| **Active** | `Type=Dial` | | | |
| **ActiveConference ActiveConference Consult** | `Type=Function` | Hold | | |
| **Active** | | Transfer | | |

*Table continues…*

| Primary Call Appearance State | Soft key setting | Action | Label | Additional parameters |
|---|---|---|---|---|
| **Active**<br>**OutgoingTransfer DialingConference ActiveConference Dialing** | | End Call | | |
| **Active**<br>**Idle**<br>**Incoming**<br>**Held**<br>**Conference Active** | | New Call | | |
| **Active** | | Conference | | |
| **Active**<br>**Held** | | Details | | |
| **Idle**<br>**Dialtone**<br>**Dialing** | | Redial | | |
| **Idle** | | Emergency<br>Night | | |
| **Incoming**<br>**Incoming Visual** | | Decline | | |

*Table continues…*

| Primary Call Appearance State | Soft key setting | Action | Label | Additional parameters |
|---|---|---|---|---|
| **Incoming**<br>**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.<br>For example:<br>`Attr1=some_address`<br>`Attr1=some_address@domain.com`<br>`Attr1=+16135555555@domain.com`<br>`Attr1=+16135555555`<br>`Attr1=16135555555`<br>`Attr1=*088063#`<br>If you do not set the value per the defined rules, the Attr1 is undefined. However, the Redirect soft key appears. |
| **Incoming**<br>**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**<br>**Conference Outgoing**<br>**Transfer Dialing**<br>**Transfer Consult** | | Cancel | | |
| **Dialing**<br>**Transfer DialingConference Dialing** | | Clear | | |

**Related links**

Configuration of soft key parameter for primary call appearance state on page 218

# 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;forced"
```

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.

| PHONEKEY setting | Allowed values | Definition | Additional parameters |
|---|---|---|---|
| **Feature** (`Type=feature`) | autocallback | Automatic Call Back | SET PHONEKEY "Key=5;Type=feature;Name=callfwd;Label=FWD" |
| | prioritycall | Priority Call | |
| | whisperpage | Whisper Paging | |
| | callpark | Call Park | |
| | callunpark | Call Unpark | |
| | callpickup | Call Pickup | |

*Table continues…*

| PHONEKEY setting | Allowed values | Definition | Additional parameters |
|---|---|---|---|
| | callpickupext | Call Pickup Extended | |
| | callpickupdir | Call Pickup Directed | |
| | cpblock | Calling Party Blocked | |
| | cpunblock | Calling Party Unblocked | |
| | callwaiting | Call Waiting | |
| | mct | Malicious Call Trace | |
| | onetouchrecording | One-Touch Recording | |
| | transfervm | Transfer to Voicemail | |
| | sac | Send All Calls | (Optional) If defined, `attr1` specifies another phone extension which this feature will manage:<br>`SET PHONEKEY "Key=1;Type=feature;Name=sac;attr1=6837;forced"` |
| | offpbx | EC500 | |
| | extendcall | Extend Call | |
| | autoicom | Auto Intercom | (**Required**) Specify the group number and the dial code as `attr1` and `attr2` respectively:<br>`SET PHONEKEY "Key=1;Type=feature;Name=autoicom;attr1=7;attr2=3554;forced"` |
| | dialicom | Dial Intercom | (**Required**) Specify the group number as `attr1`:<br>`SET PHONEKEY "Key=1;Type=feature;Name=dialicom;attr1=5;forced"` |
| | exclusion | Exclusion | |
| | autmsgwt | Automatic Message Waiting | (**Required**) Specify the phone extension as `attr1`:<br>`SET PHONEKEY "Key=1;Type=feature;Name=autmsgwt;attr1=6837;forced"` |

*Table continues…*

| PHONEKEY setting | Allowed values | Definition | Additional parameters |
|---|---|---|---|
| | team | Team button | (**Required**) Specify the phone extension as `attr1`:<br>`SET PHONEKEY "Key=1;Type=feature;Name=team;attr1=6837;forced"` |
| | limitcall | Limit Call | |
| | callfwd | Call Forward | (Optional) If defined, `attr1` specifies another phone extension which this feature will manage:<br>`SET PHONEKEY "Key=1;Type=feature;Name=callfwd;attr1=6837;forced"` |
| | callfwdbusyna | Call Forward Busy No Answer | |
| | enhcallfwd | Enhanced Call Forwarding | (Optional) If defined, `attr1` specifies another phone extension which this feature will manage:<br>`SET PHONEKEY "Key=1;Type=feature;Name=enhcallfwd;attr1=6837;forced"` |
| | huntgroupbusypos | Hunt Group Busy position | (**Required**) Specify the Hunt Busy Group number as `attr1`:<br>`SET PHONEKEY "Key=1;Type=feature;Name=huntgroupbusypos;attr1=6;forced"` |
| | SendMpage | Send multicast page | `attr1` is a mandatory parameter, which is a multicast address defined in MP_GROUPS_TO_SEND.<br>`attr2` is a mandatory parameter, which is a port defined in MP_GROUPS_TO_SEND:<br>`SET PHONEKEY "Key=8;Type=Feature;name=SendMpage;attr1=239.0.0.0;attr2=1208;Label=Sales"` |
| | agentgreetings | Agent Greetings | Applicable for Call Center environment |
| **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 | |
| | presence | Access Presence | |
| | callpriority | Call Priority | |

*Table continues…*

| PHONEKEY setting | Allowed values | Definition | Additional parameters |
|---|---|---|---|
| | guestlogin | Guest Login | |
| | wmlbrowser | WML browser | |
| **Line** (`Type=line`) | primary | Primary line appearance | (**Required**) Specify the line appearance index as `attr1`:<br>`SET PHONEKEY "Key=1;Type=line;Name=primary;attr1=1;forced"` |
| | bca | Bridged Call Appearance | (**Required**) Specify the bridged line appearance index as `attr1` and bridge extension as `attr2`:<br>`SET PHONEKEY "Key=1;Type=line;Name=bca;attr1=1;attr2=6837;forced"` |
| **Autodial** (`Type=autodial`) | autodial | Automatic dialing of a phone number | (**Required**) Specify the phone extension as `attr1`:<br>`SET PHONEKEY "Key=1;Type=autodial;Name=autodial;attr1=6837;forced"`<br>In the Avaya Aura® environment, phone extensions for automatic dialing are configured on Avaya Aura® System Manager. |
| | busyindicator | Busy Indicator | (**Required**) Specify the monitored phone extension as `attr1`:<br>`SET PHONEKEY "Key=1;Type=autodial;Name=busyindicator;attr1=6837;label=BI6837;forced"` |

**Related links**

Busy Indicator on page 240
Pre-configuration of keys parameter on page 213

# 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 | | | | |

*Table continues…*

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| | | | 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 |
| | | | | option | onevent | go | postfield | |
| | | | | | | | setvar | |
| | | | | | | noop | | |
| | | | | | | prev | setvar | |
| | | | | | | refresh | setvar | |
| | | timer | | | | | | |

*Table continues…*

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| | 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 515
[WML browser](#) on page 292
[WML syntax specifications for Avaya J100 Series IP Phones](#) on page 515

# 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 |
| 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:<br>• access control element: `<access>`<br>• text formatting elements: `<b>`, `<big>`, `<em>`, `<i>`, `<pre>`, `<small>`, `<strong>`, `<u>`<br>• fieldset element: `<fieldset>`<br>• table elements: `<table>`, `<td>`, `<tr>` |

*Table continues…*

| Specification | External standard reference | Exception |
|---|---|---|
| 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:<br>• `IPADD`<br>• `MACADDR`<br>• `MODEL`<br>• `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.<br>If the History Stack is full, the oldest entry will be deleted before a new entry is added. | N/A | No |
| Error messages are created in the following cases:<br>• a WML file cannot be obtained.<br>• a WML file is encoded in a non-supported character encoding.<br>• A card cannot be rendered.<br>• A WML file is too large.<br>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).<br>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.<br>For more information about this attribute syntax and values, see Cascading Style Sheet support on page 529. | 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.<br>This element is not visually rendered on Avaya J100 Series IP Phones. |
| <meta> | The following attributes are supported:<br>• content: specifies a description of the name attribute.<br>• name: specifies the name portion of content and name values. | A core WML element. It is not visually rendered.<br>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. |
| <card> | The following attributes are supported:<br>• newcontext<br>The following values are allowed:<br>- true: all variable bindings and the History Stack will be cleared<br>- false (default)<br>• 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.<br>• 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.<br>• ontimer: specifies a URI to be processed when the timer expires.<br>• style<br>• title: specifies a card title. The default value is New card. | A core WML element. Equivalent to an HTML page element. |

*Table continues…*

| Element name | Attributes and values | Description |
|---|---|---|
| <template> | The following attributes are supported:<br>• onenterbackward<br>• onenterforward<br>• ontimer<br>• style | This element is used to apply do and onevent elements to all cards in a deck.<br>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. |
| <br> | Only style attribute is supported for this element. | A WML element which defines a line break. |
| <p> | The following attributes are supported:<br>• align: specifies how the content is aligned. The set alignment applies to all content except for <input> elements which always align left.<br>The following values are allowed:<br>- left (default)<br>- right<br>- center<br>• mode: specifies whether the text within the paragraph can rendered on multiple lines.<br>The following values are allowed:<br>- wrap (default)<br>- nowrap<br>• style | A WML element which defines a paragraph of the text which is rendered in a new line.<br>This element can contain the following text elements:<br>• <p><br>• <a><br>• <anchor><br>• <option> |

*Table continues…*

| Element name | Attributes and values | Description |
|---|---|---|
| <a> | The following attributes are supported:<br>• 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.<br>The value is one character which can be digits 0 – 9, '*' or '#'<br>• href: specifies the URI to be processed when the element is activated.<br>For more information about this attribute values, see URI support on page 528.<br>• style<br>• title: specified a title for the element. | This element provides a simpler alternative to an anchor element with an embedded <go> element. |
| <anchor> | The following attributes are supported:<br>• accesskey<br>The value is one character which can be digits 0 – 9, '*' or '#'<br>• style<br>• title | Enables navigation between WML cards of the same deck or a different one. |

*Table continues…*

| Element name | Attributes and values | Description |
|---|---|---|
| `<img>` | The following attributes are supported:<br>• `alt`: specifies alternative text to display if the image cannot be rendered.<br>The default value is `Image not rendered`.<br>• `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%).<br>The default value is 0 pixels.<br>• `src`: specifies the URL from which the image is obtained.<br>• `style`<br>• `vspace`: specifies the space above and below the image either in pixels (n) or as a percentage of the scroll panel height (n%).<br>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:<br>• type: a mandatory attribute. Specifies the type of the <do> element.<br>The following values are allowed:<br>- accept<br>- delete<br>- help<br>- options<br>- prev<br>- reset<br>- unknown<br>• label: specifies a label for the <do> element.<br>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.<br>• name: specifies a name for the <do> element.<br>• style | A WML element used to associate a UI element to a certain task.<br>The <do> element can be used to specify soft keys additional to default soft keys.<br>**Note:**<br>In Input mode, the **Edit** soft key is added to empty locations.<br>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):<br>• empty<br>• **Home**<br>• **Refresh**<br>• **Exit**<br>If one <do> element is specified, it is displayed on the leftmost soft key and the default soft keys are shifted to the right:<br>• first <do><br>• **Home**<br>• **Refresh**<br>• **Exit**<br>If two <do> elements are specified, they are displayed as follows:<br>(Page 1 soft keys)<br>• first <do><br>• second <do><br>• empty<br>• **More**<br>(Page 2 soft keys)<br>• **Home**<br>• **Refresh**<br>• **Exit**<br>• **More** |

*Table continues…*

| Element name | Attributes and values | Description |
|---|---|---|
| | | If three <do> elements are specified, they are displayed as follows:<br>(Page 1 soft keys)<br>• first <do><br>• second <do><br>• third <do><br>• **More**<br>(Page 2 soft keys)<br>• **Home**<br>• **Refresh**<br>• **Exit**<br>• **More**<br>If four <do> elements are specified, they are displayed as follows:<br>(Page 1 soft keys)<br>• first <do><br>• second <do><br>• third <do><br>• **More**<br>(Page 2 soft keys)<br>• fourth <do><br>• **Home**<br>• **Refresh**<br>• **More**<br>(Page 3 soft keys)<br>• empty<br>• empty<br>• **Exit**<br>• **More**<br>If five <do> elements are specified, they are displayed as follows: |

*Table continues…*

| Element name | Attributes and values | Description |
|---|---|---|
| | | (Page 1 soft keys)<br>• first <do><br>• second <do><br>• third <do><br>• **More**<br>(Page 2 soft keys)<br>• fourth <do><br>• fifth <do><br>• empty<br>• **More**<br>(Page 3 soft keys)<br>• **Home**<br>• **Refresh**<br>• **Exit**<br>• **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.<br>The following values are allowed:<br>• onenterbackward: occurs when a <prev> task is activated or when a Back operation is invoked on the History Stack.<br>• onenterforward: occurs when a <go> task is activated or when a Forward operation is invoked on the History Stack.<br>• onpick: occurs when an <option> element is selected or deselected.<br>• ontimer: occurs when a timer expires.<br>**Note:**<br>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.<br>The Avaya J100 Series IP Phones WML browser supports four standard types of WML events.<br>This element is not visually rendered. |
| <postfield> | The following attributes are supported:<br>• name<br>• 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.<br>This element is not visually rendered. |

*Table continues…*

| Element name | Attributes and values | Description |
|---|---|---|
| <go> | The following attributes are supported:<br>• href<br>• method: specifies an HTTP method used to obtain a deck.<br>The following values are allowed:<br>- post: the request data is appended to the URL.<br>- get (default): the request data is sent in the body of the request.<br>• sendreferer: if set to true, the URL of the current deck is included in the HTTP request in a Referer header.<br>The allowed values are the following:<br>- true<br>- false (default) | A task element enclosed in the <do> element.<br>This element is not visually rendered. |
| <noop> | N/A | When the <noop> element is activated, no task is performed.<br>This element is not visually rendered. |
| <prev> | N/A | When the <prev> element is activated, a Back operation is invoked.<br>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.<br>This element is not visually rendered. |

*Table continues…*

| Element name | Attributes and values | Description |
|---|---|---|
| <input> | The following attributes are supported:<br>• emptyok: specifies whether the <input> field can be empty.<br>The following values are supported:<br>- true (default)<br>- false<br>• format: specifies the data format for the input field.<br>The following values are allowed:<br>- N: a numeric character<br>- M (default): any character<br>- m: any character<br>- *f: any number of characters of the type specified by f, where f is one of the character types specified above<br>- 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<br>• <inputformat>: specifies the initial text entry mode for the input field.<br>The following values are allowed:<br>- alpha: sets the initial text entry mode to “abc”<br>ALPHA: sets the text entry mode to “ABC”<br>Alpha: sets the text entry mode to “Abc”<br>Num: sets the text entry mode to “123”<br>• 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.<br>If the value bound to the variable specified by the name attribute is not | A WML element used to obtain alphanumeric data from users.<br>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.<br>• maxlength: specifies the maximum number of characters that can be entered in the field.<br>The default value is 200.<br>• name: specifies the name of the variable that will be bound to the input string.<br>• onsubmit: specifies an absolute or a relative URL.<br>• style<br>• title<br>• type: specifies the type of the input field.<br>The following values are allowed:<br>- text<br>- password<br>• 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.<br>This element is not visually rendered. |
| <option> | The following attributes are supported:<br>• onpick: specifies the URI processed if the element is activated.<br>This attribute has a higher priority than the type set in a <onevent> element.<br>• style<br>• title<br>• 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:<br>• 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.<br>• ivalue: specifies the pre-selected <option> element.<br>• multiple: specifies whether multiple items can be selected.<br>The following values are allowed:<br>- true<br>- false (default)<br>• name: specifies the name of the variable to which the value of the selected option is bound.<br>• style<br>• value: specifies the default value of the variable defined by the name attribute. | A data collection element used to declare variables.<br>This element is not visually rendered. |
| <setvar> | The following attributes are supported:<br>• name<br>• value | A WML element used to declare variables.<br>This element is not visually rendered. |
| <timer> | The following attributes are supported:<br>• name<br>• value | Declares a timer in a WML card.<br>This element is not visually rendered. |

**Related links**

Nesting of WML elements on page 513
URI support on page 528
Cascading Style Sheet support on page 529
WML browser on page 292
Nesting of WML elements on page 513

## 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.

**Related links**

WML syntax specifications for Avaya J100 Series IP Phones on page 515

## 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>
```

**Related links**

WML syntax specifications for Avaya J100 Series IP Phones on page 515

# Appendix B: 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 |

# 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
- Uruguay
- 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 ..... 273


## Numerics


802.1X
- Pass-thru mode ..... 110, 112
- supplicant ..... 110, 112


## A


AADS ..... 86
access
- disabling ..... 117
- enabling ..... 116
- phone administration menu ..... 116, 117
- restart the phone ..... 249
- web interface ..... 116, 117

access control and security
- security configurations ..... 307

acquiring service screen
- SIP global settings ..... 375
- SIP proxy server ..... 375

Active call shortcut keys
- configuration ..... 237
- overview ..... 237

admin menu
- access code ..... 92
- after log in ..... 92

admin menu parameters
- phone administration ..... 90

administering deskphone
- setting event logging ..... 99, 361
- Site-Specific Option Number ..... 106

administering emergency numbers ..... 87
administering phone
- 802.1X ..... 110, 112
- access code ..... 90
- admin menu ..... 90
- configuring SIP settings ..... 105
- debugging ..... 96, 360
- group identifier ..... 98
- IP configuration ..... 92
- IPv4 settings ..... 92
- phone startup ..... 90
- reset to defaults ..... 114
- resetting system values ..... 114
- restarting phone ..... 104
- update info ..... 109
- viewing parameters ..... 107

administration method ..... 35
administration methods
- precedence ..... 35

administration of SIP phones
- Communication Manager ..... 84
- Session Manager ..... 85

administrative methods
- file server address ..... 32
- provisioning server ..... 32

adminstering deskphone
- Ethernet interface control ..... 97

Agent greeting ..... 235
Agent Greetings
- parameters ..... 235

Always Favorites on Button Module ..... 211
assigning
- codec priority ..... 153

automatic
- settings update ..... 369
- software update ..... 369

Automatic Callback ..... 236
- configuration ..... 236

automatic failback
- DHCP request ..... 64

automatic update
- phone settings ..... 369
- phone software ..... 369

Avaya support website ..... 382


## B


best practices
- installing the phone ..... 367

Busy Indicator
- overview ..... 240

button modules ..... 296
- wall mounting ..... 29


## C


Calendar
- configuration ..... 230

Calendar integration ..... 238
call bridge on multiple devices
- phone administration ..... 263

call decline
- decline ..... 241

Call decline policy
- incoming call ..... 240

call forward generic
- web interface configuration ..... 242, 272

call log
- encryption ..... 234

call recording
SETTINGS ..... 243
Calling party number blocking ..... 243
Calling party number unblocking ..... 243
capture
phone network traffic ..... 184, 366
certificate
configuration ..... 316, 326
delete ..... 320
re-issue ..... 323, 377
renewal ..... 323, 377
replacement ..... 323
certificate management
security configurations ..... 308
certificate re-issuance
common errors ..... 377
certificate replacement errors
fixes ..... 377
changing
password ..... 119, 120, 179
phone administrator ..... 179
Changing protocol ..... 95
checklist
hardware setup ..... 23
post installation ..... 373
setup without DES ..... 37
software setup ..... 23
Codec
priority ..... 153
collection
delete ..... 380
edit name ..... 380
generating PDF ..... 380
sharing content ..... 380
Communication Manager
administration of SIP phones ..... 84
computer VLAN
full VLAN separation mode ..... 64
no VLAN separation mode ..... 64
configuration
DHCP ..... 47
Softkey sets ..... 201
Configuration
Avaya J100 Wireless Module ..... 26
configuration parameters ..... 238
Configure voicemail number ..... 291
configuring ..... 239
certificates ..... 185
Environment Setting ..... 191
Exchange Calendar ..... 195
management settings ..... 176
pre-configuration of keys ..... 199
settings ..... 153
softkey ..... 202
Configuring ..... 315
certificates ..... 313, 314
date and time ..... 174
Configuring *(continued)*
IP settings ..... 133
network ..... 124
SIP settings ..... 142
configuring Configuring
Background ..... 192
Screen Saver ..... 192
Configuring feature destination target ..... 250
configuring Group list ..... 233
configuring JEM24 background images
using web interface ..... 301
configuring JEM24 screen saver images
using web interface ..... 301
configuring presence ..... 273
configuring provision server
file server address ..... 32
configuring Voicemail ..... 291
configuring Wi-Fi network
Using phone UI ..... 104
Contacts list ..... 232
configuration ..... 233
content
publishing PDF output ..... 380
searching ..... 380
sharing ..... 380
sort by last updated ..... 380
watching for updates ..... 380
controllers ..... 87
Copy phone reports to USB flash drive ..... 289
Copying phone reports ..... 289
countries ..... 538
country list ..... 538
Cross-upgrade ..... 94
CSS support ..... 529
customization mode: parameters ..... 212
customization modes ..... 210
Customizing ringtones ..... 279

## D

dark mode
screen brightness ..... 271
Date ..... 58
debugging
web interface ..... 180, 362
deployment process
initial setup and connectivity ..... 36
DES ..... 315
mutual authentication support ..... 33
provisioning server ..... 33
Device Enrollment Server
disabling DES ..... 34
Device Enrollment Service
overview ..... 31
phone installation ..... 32, 60
device upgrade
process ..... 368

DHCP
configuration ..... 47
Option 43 codes ..... 52
option configuration ..... 49
DHCP lease
DHCPSTD ..... 52
DHCP server
configuration ..... 46
DHCP server configuration ..... 46
dial plan setting ..... 99
Digit mapping
configuration ..... 247
overview ..... 244
display
secondary ..... 16
DNS lookup ..... 76
DNS resolution
FQDN ..... 76
do not disturb
send all calls ..... 283
document changes ..... 14
documentation center ..... 380
finding content ..... 380
navigation ..... 380
documentation portal ..... 380
finding content ..... 380
navigation ..... 380
download and save the software ..... 39
downloadable ringtones ..... 279

## E

enabling
restart the phone ..... 248
enhanced local dialing
prepend a number ..... 101
Ethernet interface control
Ethernet setting ..... 97
PC Ethernet setting ..... 97
Exchange authentication
basic ..... 79
OAuth ..... 79
Exchange credential
Microsoft ..... 79
expansion module
upgrade overview ..... 302
upgrading ..... 302
Expansion module
overview ..... 296
Extension to cellular
EC500 ..... 249
external switch port
VLAN ..... 63

## F

Feature
Feature *(continued)*
do not disturb ..... 283
Send All Calls ..... 283
feature administration
Automatic Callback configuration ..... 236
Contacts list configuration ..... 233
guest login configuration ..... 253
SAC icon configuration ..... 284
team button parameters ..... 286
Voicemail configuration ..... 291
Feature administration
Calendar ..... 230
calendar configuration ..... 80, 95, 230
contacts configuration ..... 80
MLPP ..... 266
MLPP configuration ..... 266
feature configuration
Exclusion ..... 250
Feature ivocation target ..... 250
Feature target selection ..... 250
features
applications ..... 228
Call Forward ..... 241
Call Park ..... 242
Call Pickup ..... 242
Call pickup extended ..... 242
call recording ..... 243
Enhanced Call Forward ..... 241
guest login ..... 253
Recents ..... 234
Features
Presence ..... 273
field description
Exchange Calendar ..... 196
management settings ..... 176
network settings ..... 125
QoS settings ..... 139
SIP settings ..... 143
web server settings ..... 141
Field description
status ..... 121
web interface ..... 121
field descriptionfield description
Background Image ..... 192
Screen Saver ..... 192
field descriptions
certificates ..... 185
Ethernet settings ..... 134
settings ..... 154
field descriptions, debugging ..... 180, 362
file server
configuring ..... 43
finding content on documentation center ..... 380
FIPS
FIPS mode ..... 334
FIPS mode
security configurations ..... 333

## G


Generate phone report ..... 289
Generating phone report ..... 289
Group identifier ..... 98
groups
    Call pickup directed ..... 242
guest login
    configuration ..... 253


## H


hotline ..... 254
Hunt Group Busy ..... 254


## I


icom
    autoicom ..... 254
    dialicom ..... 254
identifying
    device type ..... 31
identity certificates
    security configurations ..... 309
IEEE 802.1X
    overview ..... 110
initial setup and connectivity
    deployment process ..... 36
    phone setup ..... 37
initialize
    phone ..... 41
Installed certificates ..... 325
intercom
    automatic intercom ..... 254
        intercom
            dial intercom ..... 254
IP configuring
    802.1Q ..... 93
    DNS server ..... 93
    gateway ..... 93
    HTTP server ..... 93
    HTTPS server ..... 93
        IP configuring
            Auto Provisioning ..... 93
    IPV4 setting ..... 93
    IPV6 setting ..... 93
    mask ..... 93
    phone IP address ..... 93
    SNTP sever ..... 93
    use DHCP ..... 93
    VLAN ID ..... 93
    VLAN test ..... 93
IPv4 and IPv6 operation
    overview ..... 70
IPv4 configuration
    Administration menu ..... 71
    web interface ..... 71
IPv6 configuration
    Administration menu ..... 74
    web interface ..... 75
IPv6 operation
    configuration parameters ..... 72
    DHCPv6 configuration ..... 75
    limitations ..... 76


## J


J100 Series IP Phone models ..... 15
JEM24 background image
    configuration parameters ..... 298
    JEM24 screen saver image ..... 297
JEM24 import
    background image ..... 298
    screen saver image ..... 298
JEM24 screen saver image
    configuration parameters ..... 298


## K


keys customization restoration ..... 216


## L


language ..... 209
LDAP Directory
    configuration ..... 256, 257
limitations
    Branch Session Manager ..... 349
    non-Avaya Aura proxy ..... 349
    Session Manager ..... 349
list of countries ..... 538
LLDP
    overview ..... 53
    TLV impact ..... 55
    transmitted LLDPDU ..... 54
LNCC ..... 255
logging in to
    web interface ..... 118
logging out of
    web interface ..... 118
loss of connection
    detection ..... 346
    phone ..... 346
    SIP proxy ..... 346


## M


maintenance
    downloading software upgrades ..... 40
Maintenance
    contents of the settings file ..... 207
Malicious call trace ..... 270
MDA

MDA *(continued)*
IPv4 and IPv6 ..... 264
shared control ..... 265
Microsoft exchange
authentication ..... 80
MLPP
configuration ..... 266
Multicast Paging
configuration
settings file parameters ..... 268
web UI parameters ..... 197
overview ..... 268
web UI field description ..... 198
Multiple
certificate ..... 313
certificates ..... 315
multiple identity certificate ..... 311, 313
Multiple identity certificates ..... 316, 320
My Docs ..... 380

## N

network
VLAN ..... 60
Network progress tones ..... 538
night mode ..... 271
no hold conference ..... 271
non-Avaya environment
FQDN ..... 357
redundancy ..... 357

## O

OCSP trust certificates
security configurations ..... 325
off-hook alert ..... 272
Option 43 codes
DHCP ..... 52
option configuration
DHCP ..... 49
overview ..... 272
Avaya J100 Series IP Phones ..... 15
LLDP ..... 53
Overview
Bluetooth ..... 16
Wi-Fi ..... 16

## P

parameter ..... 250
parameters
long-term acoustic exposure protection ..... 255
restart the phone ..... 248
Parameters ..... 241, 243, 280, 316, 320, 326, 334
Wi-Fi ..... 502
password
web interface ..... 119, 120
periodic check
phone settings ..... 369
phone software ..... 369
settings update ..... 369
software update ..... 369
personal profile manager ..... 86
phone
boot-up ..... 31
configuring ..... 40, 208
debugging ..... 184, 366
lock ..... 305
network traffic ..... 184, 366
unlock ..... 305
wall mounting ..... 27
phone administration
admin menu parameters ..... 90
call bridge on multiple devices ..... 263
Phone certificates ..... 325
phone configuration
administration menu ..... 89
methods ..... 89
settings file ..... 206
web interface ..... 115
phone installation ..... 31, 34
phone lock
parameters ..... 306
Phone report ..... 289
phone setup
initial setup and connectivity ..... 37
PHONEKEY
values ..... 510
ports
received packets ..... 68
TCP ..... 68
transmitted packets ..... 69
UDP ..... 68
Power management ..... 20
PPM ..... 86
user profile backup ..... 358
user profile parameters ..... 358
pre-configuration
fields ..... 200
pre-configuration of keys
configuration ..... 213
overview ..... 212
phonekey labels ..... 215
viewing internal parameter details ..... 216
preinstallation data gathering ..... 38
prerequisites ..... 34
hardware ..... 34
software ..... 35
preserved call
call forward ..... 349
call transfer ..... 349
FNU invite ..... 349

preserved call *(continued)*
limitations ... 349
Prioritization of codecs
configuration ... 276
overview ... 276
Priority Call ... 276
configuration ... 277
feature administration ... 277
Priority Call configuration ... 277
Priority order ... 313
process
device upgrade ... 368
protection
long term protection ... 255
protocols
received packets ... 68
transmitted packets ... 69
provisioning server ... 32
provisioning server configuration ... 44, 251, 252
server ... 44, 251, 252
proxy server ... 87
Public CA Certificates ... 530
Push
overview ... 277
parameters ... 278

## R

received packets
ports ... 68
protocols ... 68
redundancy
acquiring service ... 351
phone ... 346
preserved call ... 351
registrar ... 87
related documentation ... 378
Remove certificate profile ... 320
resetting
Phone to default ... 206
restart
login screen ... 249
restoring
failback ... 347
ringtones ... 279
Ringtones ... 280

## S

SAC icon
configuration ... 284
web interface configuration ... 283
SCEP certificate ... 313
screen
web interface ... 120
Scrolling mode
configuration ... 282
Scrolling mode *(continued)*
Limitations ... 283
overview ... 282
searching for content ... 380
secure installation
parameters ... 330
Secure mode
restrictions ... 345
Secure Push
overview ... 277
secure syslog
overview ... 344
parameters ... 344
security ... 304
security configuration
GDPR ... 341
Secure mode ... 341, 342
security configurations
access control and security ... 307
certificate management ... 308
FIPS mode ... 333
identity certificates ... 309
Key Usage ... 326
OCSP trust certificates ... 325
overview ... 304
trusted certificates ... 324
Selection of a higher priority line ... 285
server configuration ... 43
Server-initiated Update
applying settings ... 113
overview ... 284, 368
updating firmware ... 113
service observe ... 284
Session Manager
administration of SIP phones ... 85
Branch Session Manager ... 346
SETTINGS ... 241
settings file
configuring ... 40, 208
Recents configuration ... 234
settings file, Communication manager, presence ... 273
settings file, night mode, parameter ... 272
sharing content ... 380
Signaling ... 95
configuration ... 95
overview ... 94
Signaling protocol ... 94
updating ... 95
SIP phones
administration on Communication Manager ... 84
administration on Session Manager ... 85
SIP settings
SIP global settings ... 105
SIP proxy server ... 105
SLA Mon™ agent ... 376
SNTP parameters ... 58
SNTP server ... 57

soft key
available values ... 507
soft key configuration ... 217
call appearance state ... 217
parameters ... 218
primary call appearance ... 218
Softkey sets
web UI field description ... 203
software ... 22
downloading and saving ... 39
sort documents by last updated ... 380
specifications
hardware ... 17
support ... 382

## T

Target selection ... 250
TCP ports ... 68
team button
configuration ... 286
Team Button ... 286
Time
SETTINGS ... 58
Time server setting ... 57
TLV impact
LLDP ... 55
traffic
LAN port ... 61
PC port ... 61
Transfer phone reports ... 288
transmitted LLDPDU
LLDP ... 54
transmitted packets
ports ... 69
protocols ... 69
trusted certificates
security configurations ... 324

## U

UDP ports ... 68
USB flash drive
parameters ... 289
USB Flash drive
overview ... 288
USB Flash Drive ... 288
USB Headset
overview ... 287
parameters ... 287
USB keyboard
overview ... 290
parameters ... 290
USB Stick ... 288
user profile backup
PPM ... 358
user profile parameters
user profile parameters *(continued)*
PPM ... 358

## V

videos ... 381
View field description ... 107
viewing
certificates ... 325
installed certificates ... 185
IP address ... 117
Viewing,
phone configuration ... 121
status ... 121
view status ... 121
VLAN
IEEE 802.1Q ... 60
internal switch ... 61
VLAN tag ... 60
VLAN forwarding rules
802.1x frames ... 64
LLDP frames ... 64
spanning tree frames ... 64
VLAN ID
VLAN ID of zero ... 64
VLAN separation mode
full VLAN separation mode ... 62
no VLAN ... 62
VLAN settings
configure VLAN settings ... 61
VLAN tagging
automatic failback ... 64
voice VLAN
data VLAN ... 60
Voicemail
configuration ... 291
overview ... 291

## W

wall mounting ... 27
watch list ... 380
web interface
debugging ... 180, 362
default phone web interface ... 119
log out ... 118
log-in ... 118
password ... 119
restarting phone ... 206
screen layout ... 120
web interface Configuration
QoS settings ... 139
web server settings ... 140
Whisper Page ... 295
wireless module ... 26
installation ... 24
without DES ... 34

WML browser ..... 529
configuration ..... 293
element nesting ..... 513
overview ..... 292
syntax requirements ..... 515
URI support ..... 528