Installing and Administering Avaya J100 Series IP Phones

Release 4.0
Issue 2
December 2018

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). You 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”).

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.

Industry Canada (IC) Statements

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

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

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.

Power over Ethernet (PoE) Statement

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

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 EMC Directive 2014/30/EU and LVD Directive 2014/35/EU. A copy of the Declaration may be obtained from http://support.avaya.com or Avaya Inc., 4655 Great America Parkway, Santa Clara, CA 95054–1233 USA.

WiFi transmitter

- Frequencies for 2412-2472 MHz, transmit power: 17.8 dBm
- Frequencies for 5180-5240 MHz, transmit power: 19.14 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.

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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

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 suchdata in order to validate your eligibility to use the device.

Contents

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

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®, IP Office, and third-party call control 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 and 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 SIP-based phone with a monochrome display that supports single line call appearance.
J139 IP Phone	A SIP-based phone with a color display that supports four call appearances with two lines of call display.
J169 IP Phone	A SIP-based phone with a grayscale display that supports eight call appearances with four lines of call display. The phone can also support up to three button modules each supporting 24 application lines.

Table continues…

Phone model	Description
J179 IP Phone	A SIP-based phone with a color display that supports eight call appearances with four lines of call display. The phone can also support up to three button modules each supporting 24 application lines.

Hardware specifications

Avaya J100 Series IP Phones support the following hardware specifications:

Standard	J129	J139	J169	J179	JBM24	JEM24
Phone dimensions with the stand in high position	156 mm (6.1 in) Wide x 170 mm (6.7 in) Deep x 175mm (6.9 in) Tall	179 mm (7.0 in) Wide x 170 mm (6.7 in) Deep x 177mm (7.0 in) Tall	187 mm (7.4 in) Wide x 175 mm (6.9 in) Deep x 183 mm (7.2 in) Tall	187 mm (7.4 in) Wide x 175 mm (6.9 in) Deep x 183 mm (7.2 in) Tall	88.2 mm (3.4 in) Wide x 175 mm (6.9 in) Deep x 224.3 mm (8.8 in) Tall	115.5 mm (4.5 in) Wide x 175 mm (6.9 in) Deep x 173.64 mm (6.8 in) Tall
Phone dimensions with the wall mount	156 mm (6.1 in) Wide x 100 mm (3.9 in) Deep x 198 mm (7.8 in) Tall	179 mm (7.0 in) Wide x 100 mm (3.9 in) Deep x 219 mm (8.6 in) Tall	187 mm (7.4 in) Wide x 100 mm (3.9 in) Deep x 225 mm (8.9 in) Tall	187 mm (7.4 in) Wide x 100 mm (3.9 in) Deep x 225 mm (8.9 in) Tall	88.2 mm (3.4 in) Wide x 100 mm (3.9 in) Deep x 224.3 mm (8.8 in) Tall	115.5 mm (4.5 in) Wide x 100 mm (3.9 in) Deep x 173.64 mm (6.8 in) Tall
Wall mountable	Yes	Yes	Yes	Yes	Yes	Yes
Stand	Dual position	Dual position	Dual position	Dual position	Dual position	Dual position
Call appearances	1	4	8	8	N/A	N/A
Display type	Monochrome	Color	Grayscale	Color	Grayscale	Grayscale and color
Display	2.3”, 128 x 32 pixels	2.8”, 320 x 240 pixels	3.5”, 320 x 240 pixels	3.5”, 320 x 240 pixels	3.3”, 160 x 320 pixels	4.3”, 272 x 480 pixels
Dual color call indicator	0	4	8	8	24	24
Ethernet switch	Dual 10/100	Dual 10/100/1000	Dual 10/100/1000	Dual 10/100/1000	N/A	N/A
Wi-Fi support	Yes (As an optional module)	No	No	Yes (As an optional module)	N/A	N/A

Table continues…

Standard	J129	J139	J169	J179	JBM24	JEM24
Softkeys call control	3	4	4	4	N/A	two paging buttons
Wired Handset	Yes	Yes	Yes	Yes	N/A	N/A
Amplified Handset mode	Yes, with 20dB of gain	Yes, with 20dB of gain	Yes, with 20dB of gain	Yes, with 20dB of gain	N/A	N/A
Wired Headset	No	Yes	Yes	Yes	N/A	N/A
Expansion module capable	No	No	Yes (3)	Yes (3)	N/A	N/A
Optional DC Power	No	Yes	Yes	Yes	N/A	N/A
GSPPoE power adapter	Yes	Yes	Yes	Yes	N/A	N/A

Power specifications

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

Avaya J100 Series IP Phones are ENERGY STAR® compliant.

Important:

- J129 and J179 phones support Wi-Fi module.
- J139 is a single-class phone and does not support peripherals.
- J169 and J179 phones support JBM24 and JEM24 button modules. You can connect a maximum of three button modules of the same model simultaneously.

  Note:

  The simultaneous connection of different button module types is not supported.
- For J169 and J179 phones, use power adapter when you connect more than two button modules.
- If you are using the power adapter, disable PoE on the Ethernet connection.

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

Phone model	Avaya standard power measurements (in Watts)			Energy Star values (in Watts)
	Conservation	Typical	Maximum	Stand by
J129	2.20	2.73	3.45	1.04
J139	1.40	1.67	2.24	1.55

Table continues…

J169	1.72	1.84	2.34	1.85
J179	1.74	2.10	2.71	1.85
JBM24	0.19	0.69	1.35	NA
JEM24	1.70	1.90	2.00	NA
BT/Wi-Fi module	NA	NA	0.90	NA
BT only	NA	NA	0.10	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 without any peripheral. • IEEE 802.3af PoE Class 2 with a Wi-Fi module.
J139	• IEEE 802.3af PoE, Class 1 device.
J169	• IEEE 802.3af PoE Class1 without button module. • IEEE 802.3af PoE Class 2 for up to two button modules. • 5V DC adapter for three button modules.
J179	• IEEE 802.3af PoE Class1 without Wi-Fi module or button module. • IEEE 802.3af PoE Class 2 for up to two button modules. • 5V DC adapter for three button modules. **Note:** Use 5V DC adapter if you simultaneously connect a Wi-Fi module along with one or more button modules.

Supported codecs

Avaya J100 Series IP Phones supports the following codecs and call control protocol:

Codecs	J129	J139	J169	J179
Call control protocol	SIP	SIP	SIP	SIP
Codecs	• G.711a • G.711µ • G.729	• G.711a • G.711µ • G.729	• G.711a • G.711µ • G.729	• G.711a • G.711µ • G.729

Table continues…

Codecs	J129	J139	J169	J179
	• G.729a • G.729ab • G.726 • G722 • OPUS	• G.729a • G.729ab • G.726 • G722 • OPUS	• G.729a • G.729ab • G.726 • G722 • OPUS	• G.729a • G.729ab • G.726 • G722 • OPUS

Safety instructions

When using Avaya J100 Series IP Phones, always adhere to the following safety precautions to reduce the risk of fire, electric shock, and injury to persons.

- Read and understand all instructions.
- Follow all warnings and instructions marked on the phone.
- Do not immerse Avaya J100 Series IP Phones in water and do not use the phone when you are wet. If you accidentally drop the phone into water, do not retrieve it until you have first unplugged the line cord from the modular wall jack. Then call service personnel to ask about a replacement. Never spill liquid of any kind on the phone. If liquid is spilled, however, refer servicing to proper service personnel.
- Do not use Avaya J100 Series IP Phones during electrical storms in your immediate area to prevent the risk of electric shock from lightning. Keep urgent calls brief. In spite of protective measures to limit electrical surges, absolute protection from lightning is impossible.
- Report suspected natural gas leak immediately, but use a telephone away from the area in question. The phone’s electrical contacts could generate a tiny spark, which could ignite heavy concentrations of gas.
- Never push objects of any kind into Avaya J100 Series IP Phones through housing slots. The objects may touch hazardous voltage points or short out parts resulting in electric shock.

Button modules overview

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

Note:

The button modules are supported only by Avaya J169/J179 IP Phones.

JBM24 Button Module provides 24 additional lines for incoming calls, outgoing calls, autodialing, and calling features. The Avaya J100 Expansion Module provides 72 additional lines.

You can connect up to three button modules to Avaya J100 Series IP Phones. Each button module can be placed in both stand and wall mount positions together with the phone.

Important:

Hot plugging is not supported in Avaya J100 Expansion Module. 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 JBM24 Button Module / Avaya J100 Expansion Module:

Button modules	Call lines / Features / Applications	Switching between pages
1	24 / 72 (24 on each page)	No / Yes
2	24	No
3	24	No

Note:

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

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. For more information about downloading and extracting a software distribution package, see Downloading and saving the software on page 101.

During the boot-up, the phone will download the new firmware for the Avaya J100 Expansion Module. The `Updating software` notification will be displayed.

After the phone downloads the expansion module firmware, the upgrade process will continue in the background. The **Upgrading** status is displayed in **Main Menu** > **Administration** > **View** > **Button modules**.

The upgrade procedure for an Avaya J100 Expansion Module takes up to 4 hours for each attached module. During this time, the expansion module is operable, you can make and receive calls with it and have access to other functionality.

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"`. Press the corresponding line button for **Apply now** or **Apply tonight** option to select the suitable upgrade time.

Note:

When the Upgrade notification is displayed, the expansion module screen saver is disabled and the backlight is not turned off.

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 https://support.avaya.com/ website. See Downloading and saving the software on page 101 for more details.

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.

Debugging the expansion module

Avaya J100 Expansion Module log files contain all messages that are sent to and received from the phone. You can view the log files to monitor the user's actions on the expansion module like configuring labelled keys, making and receiving calls, enabling and disabling features, etc.

Note:

The maximum size of Avaya J100 Expansion Module log file is 5 Mb. When this size is exceeded, a `bak` prefix is added to its file name, for example, `BMLog_bak.txt`. The initial `.txt` file is cleared and writing starts from the beginning.

The log files can be generated using bm_cli debug tool which can be accessed through the phone command line.

Note:

An SSH connection must be established via an SSH client to access the phone command line. For more details, contact Avaya support at https://support.avaya.com/.

Important:

To generate log files, set log categories and levels, connect Avaya J100 Expansion Module to the phone. If the expansion module is not connected, you will get the following error message: `"Phone doesn't have JEM24 with specified id"`.

The following table shows the list of commands available through the bm_cli debug tool:

Command	Description
`help`	To print bm_cli help.

Table continues…

Command	Description
create_authfile	To install and activate `authfile.txt`. Specify the expansion module ID, for example: **create_authfile 1** **Note:** By default, the expansion modules are numbered in the order as they are connected to the phone, i.e.: 1, 2, 3.
get_file	To retrieve the specified file. Specify the expansion module ID and the path for the file you want to retrieve, for example: **get_file 1 "/AvayaDir/var/log/bm/ avaya_phone.log.1.gz"** Use **-c** argument to activate GZIP compression. **Note:** Add **/bm** to the file path as set in the example to ensure no empty files are created.
list_files	To view the list of log files of the selected expansion module in the specified directory, for example: **list_files 1 "/AvayaDir/var/log"**
remove_authfile	To deactivate `authfile.txt` for the selected expansion module, for example: **remove_authfile 1**
set_log_category	To set a log category for the selected expansion module, for example: **set_log_category 1 AUDIO** **Note:** The full list of available log categories and their description is provided in your `46xxsettings.txt` file. View allowed values for the LOG_CATEGORY parameter.
set_log_level	To set a log level for the selected expansion module, for example: **set_log_level 1 0** **Note:** The full list of available log levels and their description is provided in your `46xxsettings.txt` file. View allowed values for the LOCAL_LOG_LEVEL parameter.

Table continues…

Command	Description
`trigger_phone_report`	To generate a log report for the selected expansion module, for example: `trigger_phone_report 1`

Chapter 3: Phone installation

Hardware setup

Wi-Fi overview

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

You can configure Wi-Fi network by:

- Setting Wi-Fi parameters by using the `46xxsettings.txt` file
- Configuring Wi-Fi from the phone UI
- Configuring Wi-Fi parameters from the web UI

Note:

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

J100 wireless module

Avaya J129 IP Phone and Avaya J179 IP Phone support wireless module. The wireless module is an optional component and you can order this module separately.

Note:

Avaya J139 IP Phone and Avaya J169 IP Phone do not support J100 wireless module.

Installing the wireless module

Before you begin

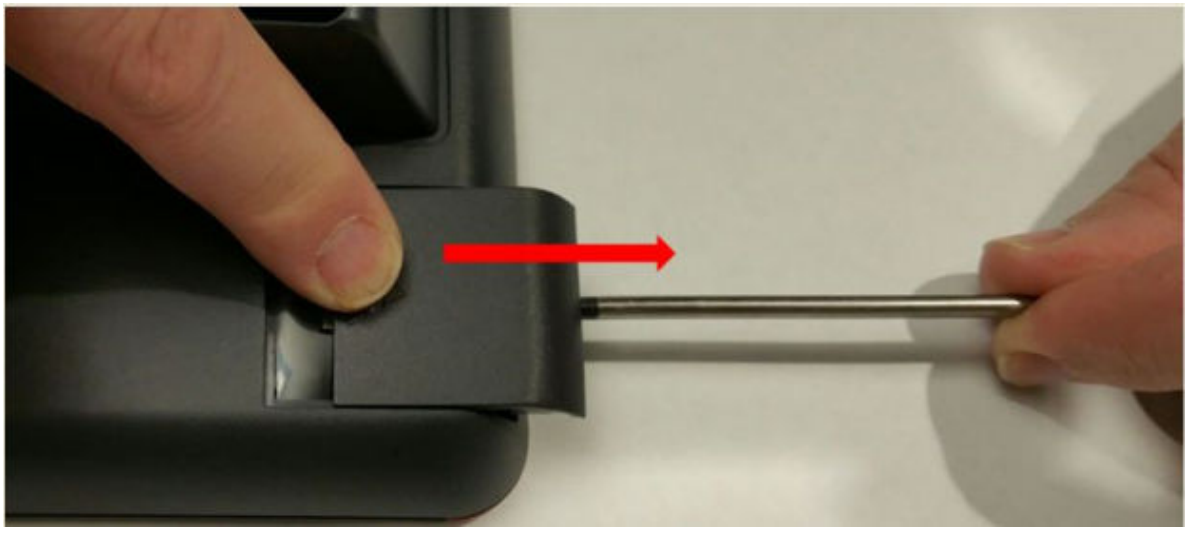
Obtain the following items:

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

Procedure

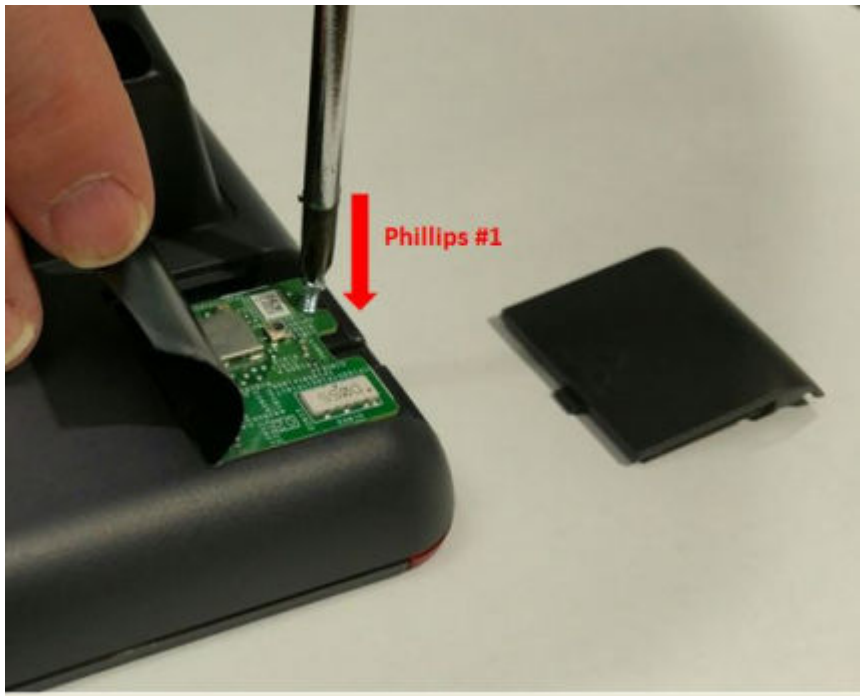
1. Insert the screw driver in the opening of the module panel to release the latch. Do not pry open the panel.

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



3. Insert the 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.

Configuring Wi-Fi using phone UI

About this task

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

Procedure

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

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

List of Wi-Fi configuration parameters

Parameter Name	Default Value	Description
WIFISTAT	`1`	Specifies the network interface to be used for network connectivity. Value operation: • `0`: Phone connects to only Ethernet network. • `1`: Phone connects to Ethernet network, unless manually switched to Wi-Fi • `2`: Phone connects to the Wi-Fi network with the SSID defined

Table continues…

Parameter Name	Default Value	Description
		in the `46xxsettings.txt` parameter WLAN_ESSID
ENABLE_NETWORK_CONFIG_BY_USER	`1`	Enables network configuration to be modified by the user. Value operation: • `0`: Disabled • `1`: Enabled
WLAN_ESSID	N/A	Specifies the wireless network to be used. The name of the SSID ranges up to 32 characters.
WLAN_SECURITY	none	Specifies the security standard to be used for the wireless network. Value operation: • none: No security standard is defined. • `wep`: WEP security standard is defined. • `wpa2psk`: WPA2 security standard with pre-shared key is defined. • `wpapsk`: WPA security standard with pre-shared key is defined. • `wpa2e`: WPA enterprise security standard is defined.
WEP_DEFAULT_KEY	N/A	Specifies the index of WEP default key. Value operation: • `1` • `2` • `3` • `4`
WLAN_COUNTRY	`US`	Specifies the ISO country code representing the Wi-Fi regulatory domain.
WLAN_ENABLE_80211D	`0`	Enables the phone to configure its Wi-Fi regulatory domain to match the 802.11d.

Table continues…

Parameter Name	Default Value	Description
		Value operation: • `0`: Disable • `1`: Enable
WEP_KEY_LEN	`128 bit`	Specifies the length of the WEP key. Value operation: • `40 bit` • `64 bit` • `128 bit`
WLAN_PASSWORD	N/A	Specifies the pre-configured Wi-Fi network password. This parameter is applicable if the WIFISTAT is enabled and WLAN_SECURITY is `wpa2psk`, or WLAN_SECURITY is `wpa2e`, WLAN_WPA2E_EAP_METHOD is `PEAP` and WLAN_WPA2E_EAP_PHASE2 is `MSCHAPV2`. The password must be from 8 to 63 characters. Note that the space and ASCII 0x20 are not supported.
WEP_KEY_1 to WEP_KEY_4	N/A	Specifies the name of the WEP key. The name of the 40 bit key and 128 bit key are of 10 hex digits and 26 hex digits respectively.
WLAN_WPA2E_EAP_METHOD	`PEAP`	Specifies the pre-configured 802.1x EAP method. This parameter is applicable if WIFISTAT parameter is enabled and WLAN_SECURITY is set as `wpa2e`. Value operation: • `PEAP` • `TLS`
WLAN_WPA2E_IDENTITY	N/A	Specifies the 802.1x name of pre-configured Wi-Fi network. This parameter is applicable if

Table continues…

Parameter Name	Default Value	Description
		WIFISTAT parameter is enabled and WLAN_SECURITY is set as `wpa2e`. The name must be from one to 32 characters. Note that the space character and ASCII 0x20 are not supported.
WLAN_WPA2E_ANONYMOUS_IDENTITY	N/A	Specifies the 802.1x anonymous name of pre-configured Wi-Fi network. This parameter is applicable if WIFISTAT parameter is enabled, WLAN_WPA2E_EAP_METHOD is set to `PEAP` and WLAN_SECURITY is set as `wpa2e`. The name must be from one to 32 characters. Note that the space character and ASCII 0x20 are not supported.
WLAN_L2QUAD	`6`	Specifies the layer 2 priority value for audio frames generated by the telephone. Valid value is from 0 to 7.
WLAN_DSCPAUD	`46`	Specifies the layer 3 Differentiated Services (DiffServ) Code Point for audio frames generated by the telephone. Valid value is from 0 to 63.
WLAN_L2QSIG	`3`	Specifies the layer 3 Differentiated Services (DiffServ) Code Point for audio frames generated by the telephone. Valid value is from 0 to 63.
SET WLAN_DSCPSIG	`34`	Specifies the layer 3 Differentiated Services (DiffServ) Code Point for signaling frames generated by the telephone. Valid value is from 0 to 63.

Wall mounting Avaya J100 Series IP Phones

About this task

The wall mounting procedure for all Avaya J100 Series IP Phones is similar. Wall mounting brackets look different for Avaya J169/J179 IP Phone and Avaya J129 IP Phone.

You can order the kit separately, using the part numbers that correspond to the phone model. For example, the part number of the wall mount bracket is 700512707. The procedure describes the wall mounting procedure with illustrations as reference.

The following procedure describes Avaya J100 Series IP Phones wall mounting with typical illustrations provided as reference.

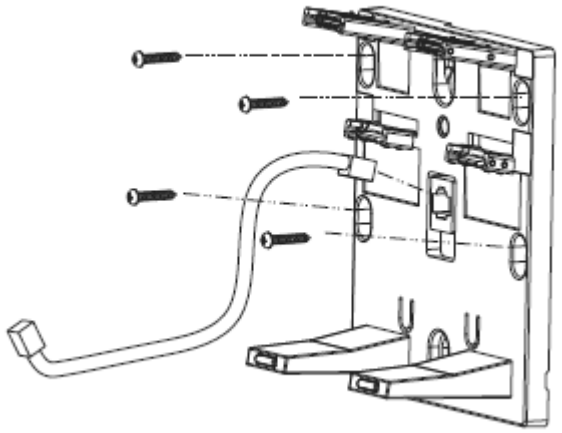
Before you begin

Obtain the following items:

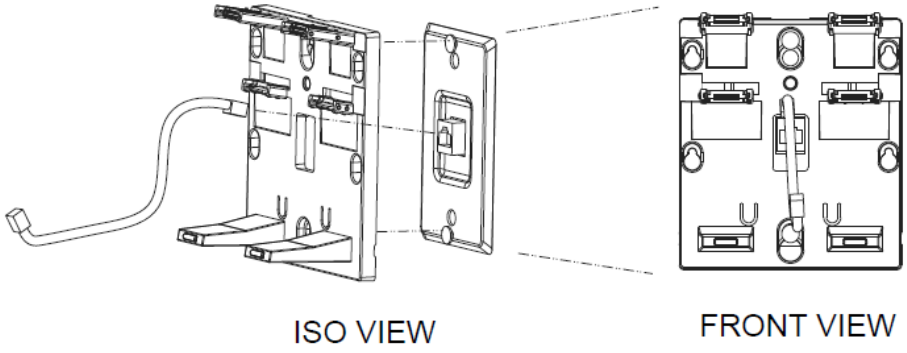
- Wall mounting kit that contains a wall mount bracket, and an Ethernet cable.
- Four #8 screws. The screws are not provided with the wall mounting kit.

Procedure

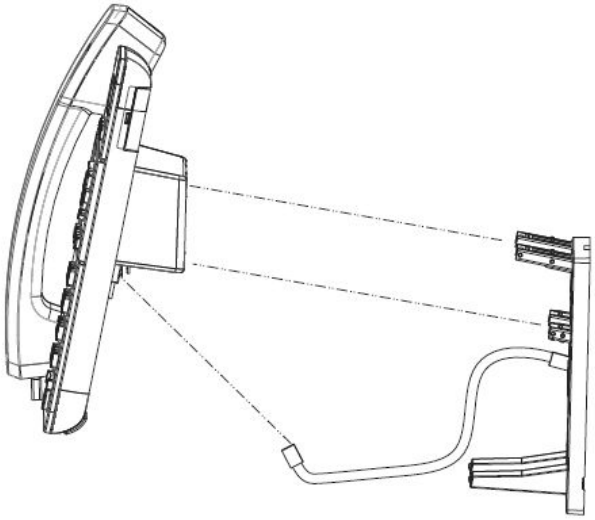
1. Do one of the following:
   - Place the bracket on the wall, drill holes, and then affix the #8 screws.



   - If there is a pre-installed wall plate, place the wall mount bracket over the wall plate. In this case, you do not need the screws.



2. Attach an Ethernet cable to the network port of the phone and to the wall jack.
3. Attach the phone to the wall mount bracket by inserting the two upper tabs of the wall mount bracket into the slots on the back of the phone. The lower pair of tabs rest against the back of the phone and ensure that the phone does not move when the keys are pressed.



Related links

Wall mounting Avaya J100 Expansion Module on page 29

Wall mounting Avaya J100 Expansion Module

About this task

Wall mounting procedure for an Avaya J100 Expansion Module is similar to the one for Avaya J100 Series IP Phones.

You can order the wall mounting bracket for Avaya J100 Expansion Module separately, along with the kit. The part number of the wall mount bracket is 700514338.

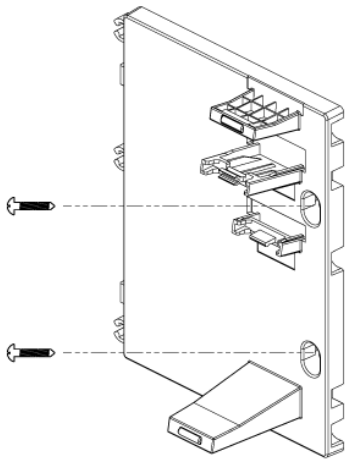
Before you begin

Obtain the following items:

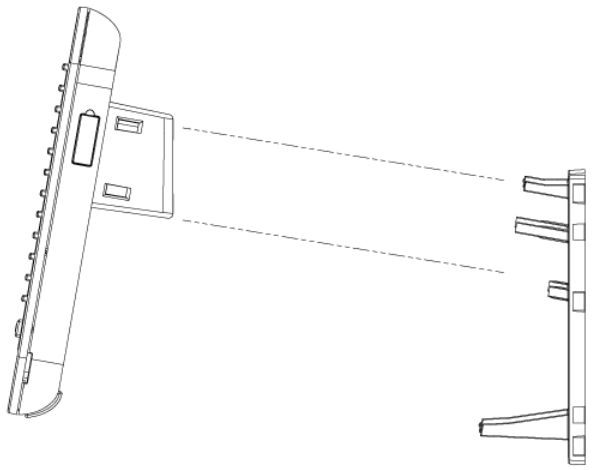
- Wall mounting kit that contains a wall mount bracket.
- Two #8 screws. The kit does not include the screws.

Procedure

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



3. Attach the Avaya J100 Expansion Module to the wall mount bracket by inserting the upper tab of the wall mount bracket into the slot on the back of the expansion module.



4. Attach the phone to the wall mount bracket. See Wall mounting Avaya J100 Series IP Phones on page 28 for more details.

Related links

Wall mounting Avaya J100 Series IP Phones on page 28

Software installation

Phone installation process

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

- With the Device Enrollment Server (DES) discovery process: The installation process begins after the phone is connected to a network. This is an automated process.
- Without the DES discovery process: The installation process includes a series of pre-configuration tasks.

Phone installation with DES

DES server

Device Enrollment Service (DES) is an Avaya cloud service used to automate the deployment of phones, especially during initial deployment. DES exposes interfaces to allow different entities to interact with the service.

Installing the phone by using DES eliminates the need for manual configuration of a provisioning server. Device Enrollment Service is available at `des.avaya.com`.

The DES phone interface

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

Installing the phone using the DES server

During initial boot-up, the phone prompts the user to select if he wants to contact the DES server. The `Do you want to activate Auto Provisioning now` notification is displayed on the phone.

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

The following options are available:

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

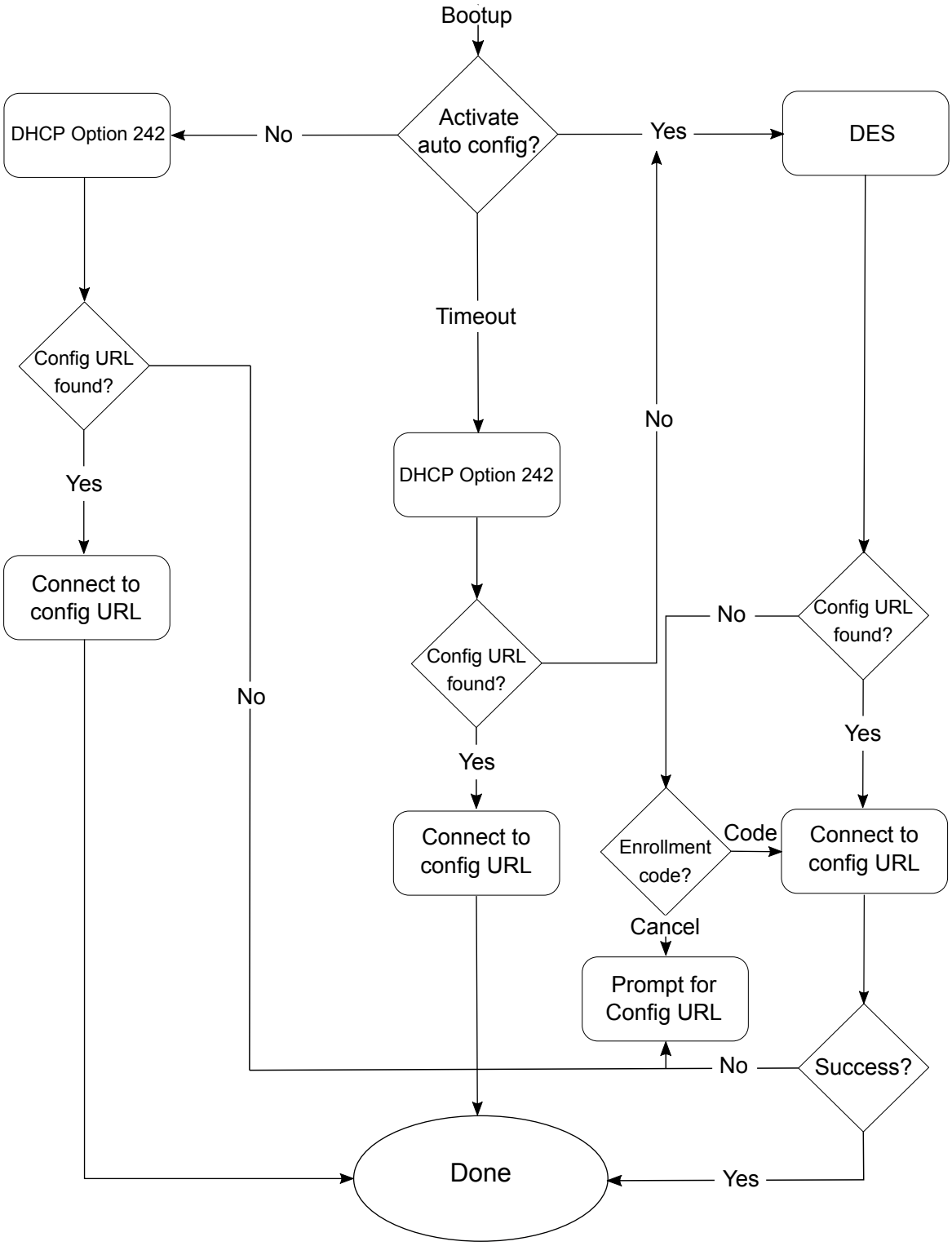
  If the phone can contact DES and is able to obtain the configuration server URL, it will contact the configuration server to get the settings. If the phone fails to contact the configuration server, it will prompt the user to enter the configuration server information manually.

  If the phone can contact DES, but there is no configuration server assigned to the phone on DES, it will prompt the user to enter the enrollment code.

  When the user enters the enrollment code, the phone will contact DES again to obtain data on its configuration server and will contact the configuration server for downloading the settings.

  The user can cancel the operation of entering the enrollment code. In this case, he will be prompted to enter the configuration server manually.
- **No**: This option indicates that the phone should not use DES and should discover the configuration server using the existing mechanism based on DHCP option 242. If the phone fails to discover the configuration server using DHCP option 242, it will prompt the user to enter a configuration server manually.
- **Timeout**: After the interval of 60 seconds, if no option is selected, the phone will use the existing mechanism based on DHCP option 242. If the phone fails to discover the configuration server in this case, it will contact DES to get the configuration server URL.

The following diagram shows the flow of DES discovery procedure:


Bootup
Activate auto config?
No
DHCP Option 242
Yes
DES
Timeout
Config URL found?
Yes
Connect to config URL
No
DHCP Option 242
Config URL found?
No
Yes
Connect to config URL
No
Config URL found?
Yes
Enrollment code?
Code
Connect to config URL
Cancel
Prompt for Config URL
No
Success?
Done
Yes

Disabling DES

During the first boot-up, the administrator can disable the DES discovery in either of the following ways:

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

Phone installation without DES

This section describes the procedure to install the phone without invoking the DES discovery process.

Initial setup checklist

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 37 for more information.	
3	Configure the servers.	See Server configuration on page 97 for more information.	
5	Configure LLDP.	See Configuration through LLDP on page 105 for more information.	
6	Configure VLAN.	See Virtual LAN (VLAN) overview on page 114 for more information.	
9	Install the phone.	See Installing the phone on page 39 for more information.	

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 Ethernet Category 5e or Ethernet Category 6 cabling
- Has one of the following specifications:
  - 802.3af PoE
  - 802.3af PoE injector

You can also power the phone using the Avaya DC 5 volt AC power adapter which you can order with the device.

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	Network Time Server	Quality of Service	Application-specific parameters
DHCP	✔	✔	✔	—	✔
LLDP	—	✔	—	✔	—
Settings file	—	✔	✔	✔	✔
Avaya Aura® System Manager and IP Office	—	—	—	—	✔
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 Settings file and DHCP when the layer 2 parameters, such as L2QVLAN, L2Q, L2QAUD, L2QVID, L2QSIG, DSCPAUD, DSCPSIG, DSCPVID, 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

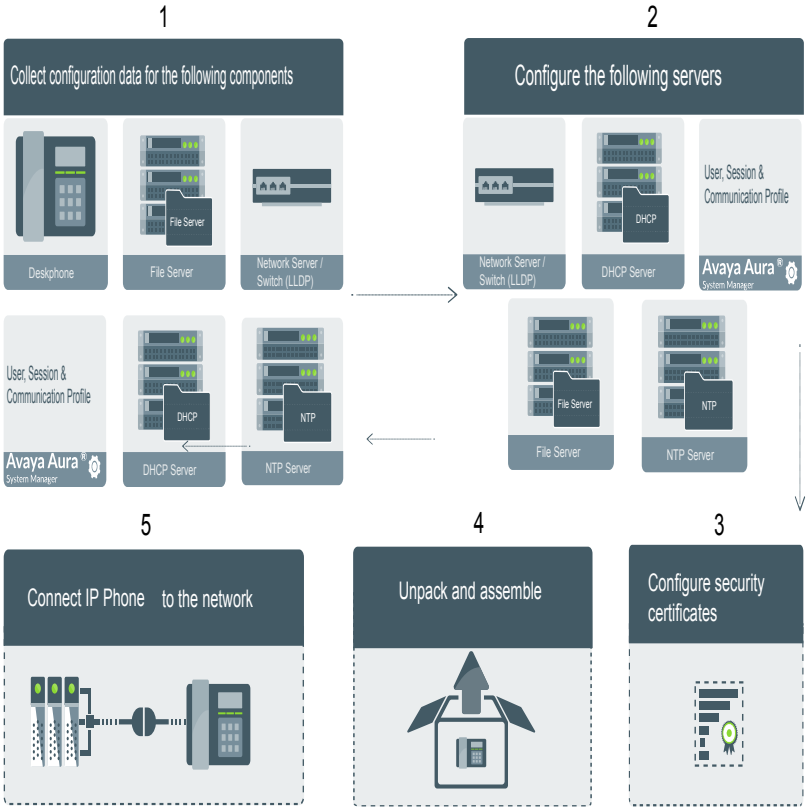
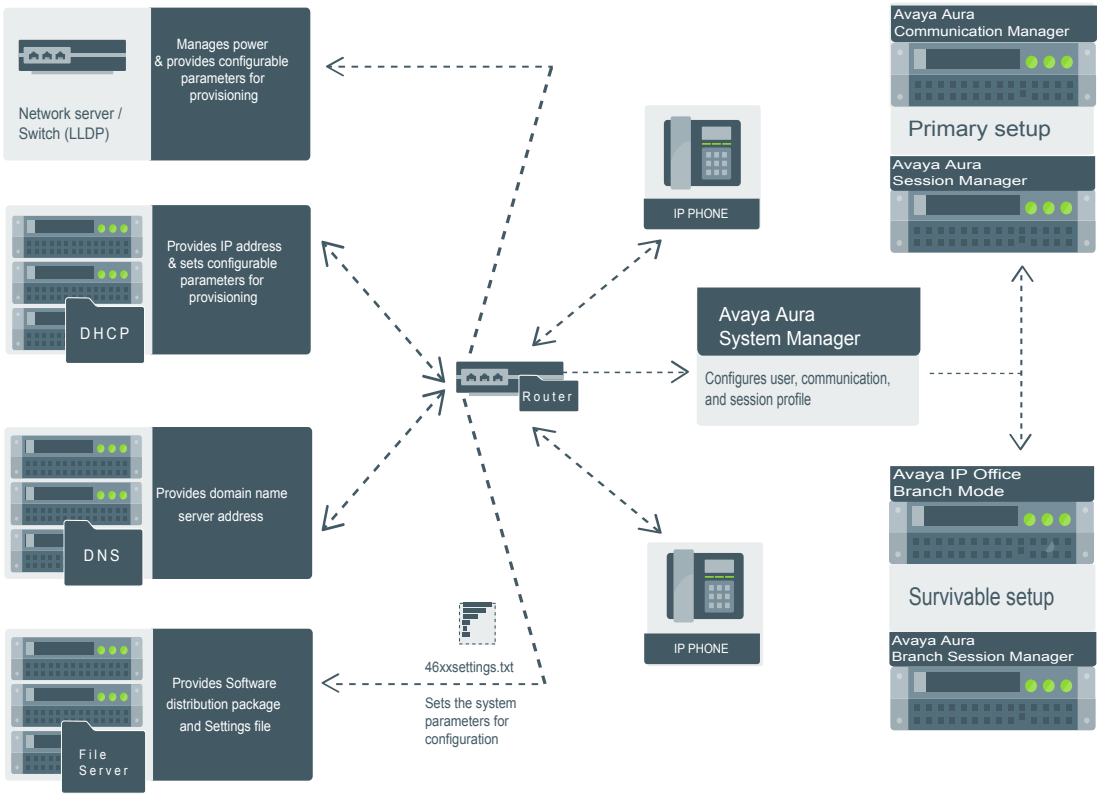


Diagram: IP phone setup



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		

Table continues…

Data for	Field	Value	Notes
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		
	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*.

Installing the phone

Before you begin

You must do the following:

- Configure the file server.
- Download and extract the firmware zip file to your file 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 checks for LLDP messages.
   b. 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 Configure Provision Server screen.
   c. In the Configure Provision Server screen, press the **Config** softkey and enter the address of the provisioning server. The provisioning server address can be in the form of IP address or a Fully Qualified Domain Name (FQDN). To enter the dot symbol (.) in the field, press the alphanumeric softkey to toggle to the alphanumeric mode.
   d. The phone verifies the VLAN ID, and starts tagging the data and voice packets accordingly.
   e. The phone sends and identifies an upgrade script file, gets the `Settings` 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** softkey for 15 seconds, and then the **Admin** and the **Login** softkeys.

        Note:

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

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

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	
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's Settings file parameters and end user settings.	List of configuration parameters on page 194	
4	Are you able to upgrade your phone?	Device upgrade process on page 189	
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 138	
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 4: Configuring the phone using 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.

Related links

Enabling access to the web interface through the Phone Administration menu on page 41
Enabling web interface access through the settings file on page 42
Viewing IP address of the phone on page 42

Enabling access to the web interface through the Phone 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 **Web Server**, and press **Select**.

   You can enable or disable access to the web interface only in third-party call control set up.
6. Scroll to **Web on HTTP**, and **Toggle** to **Yes**.
7. Press one of the following:
   - **Save**
   - **OK**

Related links

Enabling access to web interface of the phone on page 41

Enabling web interface access through the settings file

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

Parameter	Value	Description
ENABLE_WEBSERVER	1	Enables web administration of the phone.

Related links

Enabling access to web interface of the phone on page 41

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

Enabling access to web interface of the phone on page 41

Logging in and logging out of the web interface

About this task

Use this procedure to log in or log out of the web interface. Note that the system prompts you to change your default password only after the first log in.

Procedure

1. In your browser, enter the IP address of the phone and press **Enter**.
2. On the login page, type the following:
   - **Username**: The user name is always `admin`.
   - **Password**: The default password is `27238`.
3. Click **Login**.

   The system displays the Change Default Password dialog box.
4. In the Change Default Password dialog box, type the following:
   - **Current password**
   - **New password**
   - **Confirm password**
5. Click **Update**.

   The system displays the login page.
6. Log in by entering the username and the new password.
7. To log out of the web UI, click **Logout**.

Configuring network settings

About this task

Avaya J100 Series IP Phones display the details of the configuration fields in the Description section.

Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **Network**.
3. Configure the following areas:
   - Network
   - DNS
   - ICMP

- TCP
- TLS
- Web Server

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

Related links

Network settings field description on page 44

Network settings field description

Name	Description
Network	
Network Mode of Operation	Specifies the network mode used by the phone. The operations are: • **Ethernet only** • **Ethernet (preferred, but manual override allowed from Phone UI) (default)** • **Wi-Fi (preferred, but manual override allowed from Phone UI)**
DNS	
DNS Server	Specifies the IP addresses of the DNS servers added to the network. Valid value is IP addresses in dotted-decimal format, separated by commas without any intervening spaces. The default value is empty. **Note:** You can add up to 16 DNS servers.
DNS Domain	Specifies the domain name of the DNS server. Valid value must be in the DNS name format. The default value is empty.
ICMP	
Destination Unreachable Message Control	Specifies the type of the ICMP destination unreachable messages.

Table continues…

Name	Description
	The options are: • **No** • **Limited Port Unreachable messages (default)** • **Protocol and Port Unreachable messages**
Redirect Message Control	Specifies whether the ICMP redirect messages are processed or not. The options are: • **Yes** • **No (default)**
TCP	
Send TCP Keep Alive Message	Specifies whether the TCP/IP keep-alive messages are enabled or disabled in the system. The options are: • **Enable (default)** • **Disable**
TCP Keep Alive Time	Specifies the wait time interval in seconds of the phone before sending out the TCP keep-alive message (TCP ACK message) to the far-end. Valid value is an integer from 10 to 3600. The default option is 60 seconds.
TCP Keep Alive Interval	Specifies the TCP keep-alive packet re-transmission interval. Valid value is an integer from 5 to 60. The default option is 10 seconds.
TLS	
Use TLS Version	Specifies the TLS versions used in the network. The options are: • **1.0 and 1.2 (default)** • **Only 1.2**
Web Server	
Web Server On HTTP	Specifies whether HTTP access to the web interface is enabled or disabled. The options are: • **Yes (default)** • **No**

Table continues…

Name	Description
HTTP Listen Port	Specifies the port number of the web server when the web interface is accessed using HTTP. The valid value is an integer from 80 to 65535. The default port number is 80.
HTTPS Listen Port	Specifies the port number of the web server when the web interface is accessed using HTTPS. The valid value range is from 443 to 65535. The default port number is 443. The valid value is an integer from 443 to 65535.
Use certificate for Web Server	Specifies which server certificate will be used when the web interface is accessed using HTTPS. The options are: • **Factory Certificate (default)** • **Custom Certificate**

Related links

Configuring network settings on page 43

Configuring Ethernet settings

About this task

Avaya J100 Series IP Phones display the details of the configuration fields in the Description section.

Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **Ethernet**.
3. Configure the following areas:
   - IP Configuration
   - IPv4 Configuration
   - IPv6 Configuration
   - 802.1X Supplicant Operating Mode
   - VLAN
   - QoS
   - LLDP

- Ethernet Interface

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

Related links

Ethernet settings field descriptions on page 47

Ethernet settings field descriptions

Name	Description
IP Configuration	
IP Mode	Specifies the IP mode. The options are: • **IPv4 only** • **Dual mode (default)** • **IPv6 only**
Dual Mode Operation Preference	Specifies the preference of the operation mode. The options are: • **IPv4 (default)** • **IPv6**
Extended Re-bind Time	Specifies the time in seconds for which you can continue to use the assigned IP address after the DHCP lease expires. The valid value is an integer from 0 to 999. The default value is 60 seconds.
IPv4 Configuration	
Use DHCP	Specifies whether to enable/disable DHCP as a source in IPv4 network. The options are: • **Yes (default)**: To assign the IPv4 address automatically to your phone. • **No**: To assign the IPv4 address manually to your phone. **Note:** To assign the IP address manually, you must also configure the **IP Address**, **Subnet Mask**, and **Gateway IP Address** fields manually.
Continue to use DHCP information after lease expiry	Specifies whether the DHCP information can be used after the lease expires.

Table continues…

Name	Description
	The options are: • **Yes (default)**: To use the assigned IP address after the DHCP lease expires. • **No**: To stop using the assigned IP address after the DHCP lease expires.
IPv4 Address	Specifies the IP address of the phone. You can enter the IP address in this field. The valid value is an IP address in the dotted decimal name format. The maximum number of characters is 15.
Subnet Mask	Specifies the network mask address. To assign the network mask address manually to your phone, type the address in this field. The valid value is an IP address in the dotted decimal name format. The maximum number of characters is 15.
IPv4 Gateway	Specifies the IP address of the gateway. The valid value is an IP address in the dotted decimal name format. The maximum number of characters is 15.
IPv6 Configuration	
DHCPv6 Client Status	Specifies whether DHCPv6 Client is enabled or disabled. The options are: • **DHCPv6 client enabled (default)** • **DHCPv6 client disabled**
Use DHCPv6	Specifies whether to use DHCPv6 as a source in IPv6 network. The options are: • **Yes (default)**: To assign the IPv4 address automatically to your phone. • **No**: To assign the IPv4 address manually to your phone.
Continue to use DHCPv6 information after lease expiry	Specifies whether the DHCPv6 will comply with the IETF RFC 3155 standard and immediately stop using an IPv6 address if the address valid lifetime expires. The options are: • **Yes (default)** • **No**
IPv6 Address	Specifies the IPv6 address of the phone. Value format: eight groups of four hexadecimal digits. The default value is null.
IPv6 Link Local Address	Specifies the link local address.

Table continues…

Name	Description
	Value format: eight groups of four hexadecimal digits. The default value is null.
IPv6 Gateway	Specifies the IP address of the gateway. Value format: eight groups of four hexadecimal digits. The default value is null.
Use SLAAC	Specifies whether to use Stateless Auto-Configuration. The options are: • **Yes (default)** • **No**
Privacy SLAAC Mode	Specifies the preference for Privacy Extensions in SLAAC. The options are: • **Disabled, stable address generated from MAC** • **Stable private address (default)** • **Temporary address**
SLAAC Addresses	SLAAC (stateless auto configuration) IPv6 addresses. Value format: eight groups of four hexadecimal digits. The default value is null.
802.1X Supplicant Operating Mode	
Supplicant Operating Mode	Specifies the 802.1X supplicant operating mode. The options are: • **Disable (default)** • **Enable (responds only to unicast EAPOL messages)** • **Enable (responds to unicast and multicast EAPOL messages)**
802.1x Pass-through Operating Mode	Specifies the 802.1X pass-through operating mode. Pass-through refers to the forwarding of EAPOL frames between the phone's Ethernet line interface and the secondary PC Ethernet interface. The options are: • **Without proxy logoff (default)** • **With proxy logoff** • **Disabled**
Authentication Method	Specifies the authentication method to be used by 802.1X. The options are: • **MD5 (default)** • **TLS**

Table continues…

Name	Description
VLAN	
VLAN	Specifies whether the VLAN tagging is enabled or disabled. The options are: • **Auto (default)**: To support VLAN functionality by using the phone network. • **On**: To support the VLAN functionality by using the internal switch of the phone. • **Off**: To disable the VLAN functionality of the phone.
VLAN ID	Specifies the VLAN ID. To assign a VLAN ID, type the VLAN ID. Configure this parameter if the phone uses a different VLAN than the default data VLAN. The valid value is an integer from 0 to 4094. The default value is 0.
VLAN Separation Mode	Specifies the VLAN separation mode. The options are: • **Enabled (default)** • **Disabled**
VLAN Test - Wait Time for DHCP Offer	Specifies the wait time interval in seconds to receive a DHCPOFFER on a non-zero VLAN. The valid value is an integer from 0 to 999. The default value is 60 seconds.
PC Port VLAN ID	Specifies the VLAN ID of the computer port. The valid value is an integer from 0 to 4094. The default value is 0.
Tags to PC Ethernet Interface	Specifies whether the VLAN tags are stripped from Ethernet frames that leave the computer port. The options are: • **Do not remove** • **Remove (default)**
QoS	
Audio Priority (Layer 2)	Specifies the Layer 2 priority value for audio (RTP and RTCP) streams. 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 protocol messages. The valid value is an integer from 0 to 7. The default value is 6.
Audio DiffServ (Layer 3)	Specifies the layer 3 Differentiated Services (DiffServ) code point for audio frames generated by the phone. The valid value is an integer from 0 to 63. The default value is 46.

Table continues…

Name	Description
Signaling DiffServ (Layer 3)	Specifies the layer 3 Differentiated Services (DiffServ) code point for signaling frames generated by the phone. The valid value is an integer from 0 to 63. The default value is 34.
LLDP	
LLDP	Specifies the status of LLDP. The options are: • **Disabled** • **Enabled** • **Enabled- only if LLDP frame is received (default)**
Ethernet Interface	
Ethernet	Specifies the speed and duplex settings for the Ethernet line interface. The options are: • **Auto-negotiate (default)** • **10Mbps half-duplex** • **10Mbps full-duplex** • **100Mbps half-duplex** • **100Mbps full-duplex**
PC Ethernet	Specifies the speed and duplex settings for the secondary (PC) Ethernet interface. The options are: • **Disable** • **Auto-negotiate (default)** • **10Mbps half-duplex** • **10Mbps full-duplex** • **100Mbps half-duplex** • **100Mbps full-duplex**
PC Ethernet auto-MDIX	Specifies the status of the auto-MDIX on PHY2. The options are: • **Enable (default)** • **Disable**

Related links

Configuring Ethernet settings on page 46

Configuring Wi-Fi settings

About this task

Avaya J100 Series IP Phones display the details of the configuration fields in the Description section.

Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **Wi-Fi**.
3. Configure the following areas:
   - WiFi Control
   - WiFi Setting
   - IP Configuration
   - WEP
   - WPA2 Enterprise (802.1x)
   - QoS
4. Click one of the following:
   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.

Related links

Wi-Fi settings field descriptions on page 52

Wi-Fi settings field descriptions

Name	Description
WiFi Control	
WLAN Network Configuration Mode	Specifies the Wi-Fi network configuration mode. The options are: • **Automatic (default)** • **Manual**
WiFi Setting	
Country	Specifies the country code to define the Wi-Fi radio parameters permitted by the local regulatory domain. Value format: two-character country code. The default value is **US**.

Table continues…

Name	Description
Use of 802.11d	Configures the 802.11d specifications automatically to the local regulatory domain for the WLAN network. The options are: • **Disable (default)** • **Enable**
WLAN Active SSID	Displays active SSID when Wi-Fi is active. This is an internal parameter. Value format: a sting from 0 to 32 characters. The default value is empty.
SSID	Specifies the SSID string of the Wi-Fi network. Value format: alphanumeric characters and special symbols. **Note:** The space character (ASCII 0x20) is not supported. The default value is empty.
Security	Specifies the WLAN security standard for your Wi-Fi network. The options are: • **None (default)** • **WEP Security** • **WPA/WPA2 security (pre-shared key) security** • **WPA2 Enterprise security (802.1x auth.)**
WLAN Max Authentication Retires	Specifies the number of retries that will be attempted to establish a secure connection upon receiving authentication failures. The options are: • **0** • **1** • **2** • **3 (default)** • **4**
IP Configuration	
Use DHCP	Specifies whether DHCP is used in the Wi-Fi network. The options are: • **Yes (default)** • **No**

Table continues…

Name	Description
IP Address	Specifies the IP address of the phone. The valid value is the IP address in the dotted decimal name format. The maximum number of characters is 15. The default value is “0.0.0.0”.
Subnet Mask	Specifies the Wi-Fi network mask address. The valid value is the IP address in the dotted decimal name format. The maximum number of characters is 15. The default value is “0.0.0.0”.
Gateway IP Address	Specifies the IP address of the gateway in the Wi-Fi network. The valid value is the IP address in the dotted decimal name format. The maximum number of characters is 15. The default value is “0.0.0.0”.
WEP	
WEP Key Length	Specifies the passcode key length for WEP security. The options are: • **64 bit** • **128 bit (default)**
WEP Default Key	Specifies the default key in your Wi-Fi network. The options are: • **WEP Key 1 (default)** • **WEP Key 2** • **WEP Key 3** • **WEP Key 4**
WEP Key 1	Specifies the WEP key values in the Wi-Fi network. The valid value is up to 26 alphanumeric characters that can be the following: • Blank • 0 – 9 • A – F The value must include 10 hexadecimal digits for 64 bit keys and 26 hexadecimal digits for 128 bit keys. The default value is empty.
WEP Key 2	Specifies the WEP key values for the Wi-Fi network.

Table continues…

Name	Description
	The valid value is up to 26 alphanumeric characters that can be the following: • Blank • 0 – 9 • A – F The value must include 10 hexadecimal digits for 64 bit keys and 26 hexadecimal digits for 128 bit keys. The default value is empty.
WEP Key 3	Specifies the WEP key values for the Wi-Fi network. The valid value is up to 26 alphanumeric characters that can be the following: • Blank • 0 – 9 • A – F The value must include 10 hexadecimal digits for 64 bit keys and 26 hexadecimal digits for 128 bit keys. The default value is empty.
WEP Key 4	Specifies the WEP key values for the Wi-Fi network. The valid value is up to 26 alphanumeric characters that can be the following: • Blank • 0 – 9 • A – F The value must include 10 hexadecimal digits for 64 bit keys and 26 hexadecimal digits for 128 bit keys. The default value is empty.
WPA2 Enterprise (802.1x)	
EAP Authentication Method	Specifies the type of EAP authentication method. The options are: • **PEAP (default)** • **TLS**
EAP Phase 2 Authentication Method	Specifies the type of EAP Phase 2 authentication method. The options are: • **None (default)** • **MSCHAPV2**
Authentication Identity	Specifies the authentication identity.

Table continues…

Name	Description
	The valid value is a string of up to 32 alphanumeric characters and special symbols. The default value is blank. **Note:** The space character (ASCII 0x20) is not supported.
Password	Specifies the password for the Authentication identity. 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 blank. Value format: alphanumeric characters and special symbols. **Note:** The space character (ASCII 0x20) is not supported.
Authentication Anonymous Identity	Specifies the Authentication identity. The valid value is a string of up to 32 alphanumeric characters and special symbols. The default value is blank. **Note:** The space character (ASCII 0x20) is not supported.
QoS	
Audio Priority (Layer 2)	Specifies the Layer 2 priority value for RTP and RTCP audio streams. The options are from 0 to 7. The default value is 6.
Signaling Priority (Layer 2)	Specifies the Layer 2 priority value for signaling protocol messages. The options are from 0 to 7. The default value is 3.
Audio DiffServ (Layer 3)	Specifies the layer 3 Differentiated Services (DiffServ) code point for audio frames generated by the phone. The valid value is an integer from 0 to 63. The default value is 46.
Signaling DiffServ (Layer 3)	Specifies the layer 3 Differentiated Services (DiffServ) code point for signaling frames generated by the phone. The valid value is an integer from 0 to 63. The default value is 34.

Related links

Configuring Wi-Fi settings on page 52

Configuring SIP settings

About this task

Avaya J100 Series IP Phones display the details of the configuration fields in the Description section.

Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **SIP**.
3. Configure the following areas:
   - SIP Account
   - XSI
   - Busy Lamp Field (BLF)
   - SIP Global Settings
   - Codecs and DTMF
   - RTP
   - SRTP
   - 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.

Related links

SIP settings field descriptions on page 57

SIP settings field descriptions

Name	Description
SIP Account	
Registration Status	Displays the SIP account status. The field is automatically populated. The status can be the following: • Not Configured • Not Registered

Table continues…

Name	Description
	• Registered
SIP User ID	Specifies the SIP user ID used to log in to the phone. You can also type the SIP user ID, which is a combination of the following values: • Upper and lower case characters. • Numbers from 0 to 9. • Spaces. • Special characters. The allowed characters are the following: . , : ; “” ‘ / () {} [] ` ~ * _ ! ? + - ^ # = <> | & $ — The default value is empty.
Authentication User ID	Specifies the authentication ID. You can also type the authentication user ID in this field if authentication is enabled on the SIP server. The authentication user ID is a combination of the following values: • Upper and lower case characters. • Numbers from 0 to 9. • Spaces. • Special characters. The allowed characters are the following: . , : ; “” ‘ / () {} [] ` ~ * _ ! ? + - ^ # = <> | & $ —
Authentication Password	Specifies the authentication password. You can also type the password in this field if authentication is enabled on the SIP server. **Note:** The password can contain maximum 31 ASCII characters. The default value is empty.
XSI	
XSI State	Specifies the status of XSI. The values are: • Initializing • Success • Failure
XSI URL	Specifies the FQDN or the IP address, HTTP or HTTPS mode and the port of the XSP server. The valid value is a string of 0 to 255 ASCII characters.

Table continues…

Name	Description
XSI Event Channel Duration	Specifies the time duration in minutes for XSI event channel. The phone will ask XSP server to maintain the established Comet HTTP connection for the specified period of time. After 50% of this time phone will reestablish Comet HTTP connection. The valid value is an integer from 60 to 1440. The default value is 60 minutes.
XSI Event Channel HeartBeat	Specifies the time interval in seconds to send heartbeat messages over Comet HTTP connection to XSP server of BroadWorks. The valid value is an integer from 1 to 999. The default value is 15 seconds.
XSI User Id	Specifies the BroadSoft user ID which the phone must use for XSI authentication. BroadSoft user Id is the SIP user Id excluding at (@) and domain. The valid value is a string of 0 to 255 ASCII characters.
XSI Web Password	Specifies the BroadSoft's web portal password which the phone must use for XSI web authentication. If the value is null, SIP authentication method is used.
Busy Lamp Field(BLF)	
Allow User to Change BLF List	Specifies the control to provide the user permissions to add and remove BLF monitored users from the phone. The values are: • **User is allowed to add or delete BLF monitored users** • **User is allowed to add BLF monitored users** • **User is allowed to delete BLF monitored users** • **User is allowed to add and delete BLF monitored users (default)**
SIP Global Settings	
SIP Domain	Specifies the SIP domain used for SIP registration. The valid value is a string of 0 to 255 ASCII characters.
Enable PPM as source of Proxy Server	Specifies whether PPM is used as a source of SIP proxy server information. **Note:** This is an Avaya Aura® setting which is ignored in the 3PCC environment. The options are: • **Yes (default)** • **No**

Table continues…

Name	Description
Proxy Policy	Specifies whether SIP proxy servers are read-only or can be edited. The options are: • **Manual (Use Phone Admin Menu or WEB to configure)**: To configure SIP proxy server manually by using the phone or the web interface. • **Automatic (Can be set from DHCP, LLDP, Settings File, PPM) (default)**: To use the SIP proxy server settings received from the `46xxsettings.txt` file or PPM.
SIP Proxy Server	Specifies the SIP proxy server domain. The valid value is a string of 0 to 255 ASCII characters, for example: `148.147.158.185:5061;transport=tls,alphagreensm01.avaya.com:5061;transport=tls`
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. The options are: • **Simultaneous (default)** • **Alternate**
Number of proxy server to register simultaneously	Specifies the number of SIP proxy controllers that the phone can register simultaneously. The options are: • **1** • **2** • **3 (default)**
Registration Interval	Specifies the time interval in seconds between two registrations to the SIP proxy. The valid value is an integer from 30 to 86,400. The default value is 900 seconds.
Un-registration Wait Timer (seconds)	Specifies the time in seconds during which the phone waits before terminating all SIP dialog and SIP registrations. The valid value is an integer from 4 to 3,600. The default value is 32 seconds.
Registration Wait Timer (seconds)	Specifies the time in seconds during which the phone waits for a response message from registration. If no response message is received within this time, the phone tries to register again. The valid value is an integer from 4 to 3,600. The default value is 32 seconds.

Table continues…

Name	Description
Signaling IP Preference	This parameter is used by SIP signaling only on a dual mode phone (phone with both IPv4 and IPv6 addresses configured) to select the preferred SIP controller IP addresses. The default value is **IPv4**.
Media IP Preference	Specifies the preference of SDP media group lines and the SDP answer/offer format when phone is in dual mode. The default value is **IPv4**.
Codecs and DTMF	
OPUS	Specifies whether the OPUS codec capability of the phone is enabled or disabled. The options are: • **Disabled** • **Enabled WIDEBAND_20K (default)** • **Enabled NARROWBAND_16K** • **Enabled NARROWBAND_12K**
G.722	Specifies whether the G.722 codec is enabled. The options are: • **Disable** • **Enable (default)**
G.726	Specifies whether the G.726 codec is enabled. The options are: • **Disable** • **Enable (default)**
G.729	Specifies whether the G.729A codec is enabled. The options are: • **Disable** • **Enable without Annex B support (default)** • **Enable with Annex B support**
G.711u law	Specifies whether the G.711u law codec is enabled. The options are: • **Disable** • **Enable (default)**
G.711a law	Specifies whether the G.711a law codec is enabled.

Table continues…

Name	Description
	The options are: • **Disable** • **Enable (default)**
Send DTMF	Specifies whether the phone sends DTMF tones in-band as regular audio, or out-of-band using RFC 2833 procedures. The options are: • **In-band** • **Out-of-band (default)**
OPUS Payload	Dynamically specifies the RTP payload type to be used for OPUS codec. The parameter is used when the media request is sent to the far-end in an INVITE or 200 OK when INVITE with no Session Description Protocol (SDP) is received. The valid value is an integer from 96 to 127. The default value is 116.
G.726 Payload	Specifies the RTP payload type to be used for the G.726 codec. The valid value is an integer from 96 to 127. The default value is 110.
DTMF Payload	Specifies the RTP payload type to be used for RFC 2833 signaling. The valid value is an integer from 96 to 127. The default value is 120.
RTP	
Play Tone till RTP	Specifies whether the locally generated ringback tone stops when SDP is received for an early media session, or whether it continues until RTP is actually received from the far-end party. The options are: • **Yes (default)** • **No**
Symmetric RTP	Specifies whether the phone must receive RTP if the UDP source port number is not same as the UDP destination port number. The options are: • **Disable** • **Enable (default)**
RTCP_XR	Specifies whether VoIP Metrics Report Block as defined in RTP Control Protocol Extended Reports (RTCP XR) (RFC 3611) is sent as part of the RTCP packets to a remote peer or an RTCP monitoring server. The options are: • **Yes** • **No (default)**
SRTP	

Table continues…

Name	Description
Media Encryption	Specifies the crypto suite and session parameters for media encryption. The options are: • **aescm128-hmac80** • **aescm128-hmac32** • **aescm128-hmac80-unauth** • **aescm128-hmac32-unauth** • **aescm128-hmac80-unenc** • **aescm128-hmac32-unenc** • **aescm128-hmac80-unenc-unauth** • **aescm128-hmac32-unenc-unauth** • **none (default)** • **aescm256-hmac80** • **aescm256-hmac32** **Note:** You should not use unauthenticated media encryption (SRTP) files.
Encrypt RTCP	Specifies whether RTCP packets are encrypted or not. The options are: • **Yes**: SRTCP is enabled. • **No (default)**: SRTCP is disabled.
Enforce "SIPS" URI for SRTP	Specifies whether a SIPS URI must be used for SRTP. The options are: • **Yes (default)**: Enforced • **No**: Not enforced.
SDP Negotiation Capability	Specifies the Session Description Protocol (SDP) negotiation capability. • **Yes (default)** • **No**
Timers and Count	
SIP Timer T1	Specifies an estimate in milliseconds for the Round Trip Time (RTT). The valid value is an integer from 500 to 10,000. The default value is 500 milliseconds.
SIP Timer T2	Specifies the maximum retransmit interval in milliseconds for non-INVITE requests and INVITE responses. The valid value is an integer from 2,000 to 40,000.

Table continues…

Name	Description
	The default value is 4,000 milliseconds.
SIP Timer T4	Specifies the maximum duration in milliseconds for which a message remains in the network. The valid value is an integer from 2,500 to 60,000. The default value is 5,000 milliseconds.
INVITE Response Timeout	Specifies the maximum number of seconds that the phone waits for another response after receiving a SIP 100 Trying response. The valid value is an integer from 30 to 180. The default value is 60 seconds.
Failed Session Removal Timer	Specifies the time in seconds to automatically remove a failed call session. The valid value is an integer from 5 to 999. The default value is 60 seconds.
Outbound Subscription Duration Request	Specifies the Outbound subscription request duration in seconds. The valid value is an integer from 60 to 31,53,600. The default value is 86,400 seconds.
Controller Search Interval	Specifies the time in seconds that the phone waits to complete the maintenance check for monitored controllers. The valid value is an integer from 4 to 3,600. The default value is 16 seconds.
Active subscription wait time for "avaya-cm-feature-status"	Specifies the time in seconds that the phone waits to validate an active subscription when it subscribes to the avaya-cm-feature-status package. The valid value is an integer from 16 to 3,600. The default value is 60 seconds.
Remote Data Source initial retry time	Specifies the number of seconds that the phone waits for the first time before trying to contact the PPM server again after a failed attempt. Each subsequent retry is delayed by double the previous delay time. The valid value is an integer from 2 to 60. The default value is 2 seconds.
Remote Data Source maximum retry time	Specifies the maximum delay interval in seconds after which the phone stops to contact the PPM server. The valid value is an integer from 2 to 3,600. The default value is 600 seconds.
Remote Data Source initial retry attempts	Specifies the number of attempts the PPM adaptor must try to download from PPM before it stops connecting to the PPM server. The valid value is an integer from 1 to 30. The default value is 15 attempts.

Table continues…

Name	Description
Local Port	
RTP Port (minimum)	Specifies the lower limit of a port range. • RTP • RTCP • SRTP • SRTCP The valid value is an integer from 1024 to 65,503. The default value is 5004.
RTP Port (range)	Specifies the port range to be used by the following connections: • RTP • RTCP • SRTP • SRTCP The valid value is an integer from 32 to 64,511. The default value is 40.
SIP Signaling Port (minimum)	Specifies the lower limit of a port range to be used for SIP signaling. The valid value is an integer from 5062 to 65,503. The default value is 5062.
SIP Signaling Port (range)	Specifies the port range to be used for SIP signaling. The valid value is an integer from 32 to 60,473. The default value is 60473.
Miscellaneous	
Conference Factory URI	Specifies the URI for Avaya Aura® Conferencing or network conferencing in third-party call control environments. The valid value is a string of up to 255 ASCII characters.
Subscribe Event Packages	Specifies a comma-separated list of event packages to subscribe to after registration. Possible values are: • `reg` • `dialog` • `mwi` • `ccs` • `message-summary`, which is identical to `mwi` • `avaya-ccs-profile`, which is identical to `ccs`

Table continues…

Name	Description
	For IP Office, you must use the following: • `reg` • `message-summary`, which is identical to `mwi` • `avaya-ccs-profile`, which is identical to `ccs` For the third-part call control setup, you can use `message-summary`.
Voice Mail Access Code	Specifies the number to access the voice mail in a non-Avaya environment.
100rel	Specifies whether the 100rel option tag is included in the SIP INVITE header field. The options are: • **Disable**: The tag is not included. • **Enable (default)**: The tag is included.
Validate Incoming messages	Specifies whether AOR received in Request-URI of an incoming call must be validated with the contact header published by phone during registration. The options are: • **Disable (default)** • **Enable**
'Privacy' header in Incoming message	Specifies whether AOR received in Request-URI of an incoming call must be private in the contact header published by the phone during registration. The options are: • **Display CallerID information (default)** • **Display 'Restricted'**

Related links

Configuring SIP settings on page 57

Configuring Settings

About this task

Avaya J100 Series IP Phones display the details of the configuration fields in the Description section.

Procedure

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

3. Configure the following areas:
   - Language
   - Feature Access
   - Phone Menu Options
   - Call Log
   - Contacts
   - Emergency Call
   - Phone Lock
   - Other
   - Audio
   - Dialing
   - Enhanced Local Dialing Rules
   - Admin
   - MLPP
   - Guest Login
   - Save Extension
   - Bluetooth
   - CCMS
   - Brightness
4. Click one of the following:
   - **Save**: To save the configuration changes.
   - **Reset to Default**: To revert to the default values.

Related links

Settings field descriptions on page 67

Settings field descriptions

Language

Name	Description
Language	
Available Language File	Specifies the name of the default system language file used in the phone.

Table continues…

Name	Description
	You can delete the default language file by clicking **Delete**.
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. The valid value is a sting of up to 1024 characters. The default value is empty.
Phone Language	Specifies the language used in phone system. Value format: complete language file name from 0 to 32 characters, for example: `Korean.xml`. The default value is empty.
Feature Access	
Call Forward	Specifies the status of the Call Forwarding feature. The options are: • **Off (default)** • **Unconditional** • **Busy** • **Unconditional and Busy** • **No answer** • **Unconditional and No answer** • **Busy and No answer** • **Unconditional, No answer and Busy**
Number of Ring cycle before Call Forward	Specifies the number of ring cycles before the call is forwarded. The valid value is an integer from 0 to 20. The default number of ring cycles is 1.
Do Not Disturb	Specifies the status of the Do Not Disturb feature. The options are: • **Do Not Allow** • **Allow (default)**
DND Priority over Call Forward (Unconditional, Busy)	Specifies the priority between the Do Not Disturb and Call Forward (Unconditional/Busy) features when both are activated by the user. The options are: • **Yes** • **No (default)**
Auto Answer	Specifies the status of the Auto Answer feature.

Table continues…

Name	Description
	The options are: • **Do Not Allow (default)** • **Allow**
Mute on Auto Answer	Specifies muting when the Auto Answer feature is enabled. The options are: • **Yes (default)** • **No**
Hold Reminder Timer	Specifies the time in seconds after which the phone plays the hold reminder tone. The valid value is an integer from 0 to 999. The default value is 0 seconds.
Transfer on Conference hangup	Specifies whether a conference call continues after the host hangs up. The options are: • **Yes** • **No (default)**
Presence	Specifies the status of the Presence feature. The options are: • **Do Not Allow** • **Allow (default)**
Phone Menu Options	
Settings	Specifies whether the Settings menu is displayed on the phone. The options are: • **Do Not Allow** • **Allow (default)**
Network Info Screen	Specifies whether the Network Information screen is displayed on the phone. The options are: • **Do Not Allow** • **Allow (default)**
SIP User Logout	Specifies whether the Logout feature is provided to the user. The options are: • **Do Not Allow** • **Allow (default)**

Table continues…

Name	Description
SSL Version	Specifies the version of the SSL certificate.
UDP Transport	Specifies whether UDP transport is allowed. The options are: • **Do Not Allow (default)** • **Allow**
Network Configuration by User	Specifies whether the network configuration can be modified by the user. The options are: • **Do Not Allow to Modify** • **Allow to Modify (default)**
Call Log	
Call Log	Specifies whether to enable or disable the Call Log application on the phone. The options are: • **Do Not Allow** • **Allow (default)**
Redial Softkey	Specifies whether the **Redial** softkey is available. The options are: • **Do Not Allow** • **Allow (default)**
Redial in Phone Menu	Specifies whether phone redials the last number or displays the list of recently dialed numbers. The options are: • **Do Not Allow (default)** • **Allow**
Redial Softkey Options	Specifies whether to show a list or one number on the **Redial** softkey. The options are: • **List (Redial out of list)** • **One number (default)**
Contacts	
Local Contacts	Specifies whether to enable or disable the Contacts application on the phone. The options are: • **Do Not Allow**

Table continues…

Name	Description
	• **Allow (default)**
Contact Name Format	Specifies the format of the contact name to be displayed in the Contacts list. The options are: • **'Last Name' 'First Name' (default)** • **'First Name' 'Last Name'**
Contact Name display logic	Specifies how to match a dialed string on an incoming call with the users contacts. The options are: • **Match the number completely (default)** • **Match shorter number completely to the rightmost digits of longer number** • **Match at least 4 rightmost digits**
Emergency Call	
Emergency Numbers	Specifies the emergency contact number. **Note:** Emergency calls are not supported in the 3PCC environment.
Emergency Softkey	Specifies whether the **Emergency** softkey is displayed after the phone is registered. The options are: • **Do Not Display** • **Display without Confirmation** • **Display with Confirmation (default)**
Softkey Emergency Number	Specifies the number(s) which is dialed when the **Emergency** softkey is pressed. The valid value is up to 30 dialable characters. The default value is empty. Value format: digits from 0 to 9, *, #.
Emergency Softkey on Unregistration	Specifies whether the **Emergency** softkey is displayed when the phone is not registered. The options are: • **Do Not Display** • **Display without Confirmation** • **Display with Confirmation (default)**
Phone Lock	

Table continues…

Name	Description
Enable Phone Lock	Specifies whether the Lock feature is enabled on the phone. The options are: • **Do Not Allow (default)** • **Allow**
Phone Lock Idle Time	Specifies the idle time in minutes after which the phone is locked. The valid value is an integer from 0 to 10080. The default value is 0 minutes.
Other	
Softkey Configuration	Specifies which feature will show up on which softkey on the phone screen. **Note:** This setting applies only to Avaya J129 IP Phone. The following numbers are assigned to the features: • 0 – Redial • 1 – Contacts • 2 – Emergency • 3 – Recents • 4 – Voicemail Value format: numbers from 0 to 4 and a comma (,). The default value is “0,1,2”.
Branding Volume	Specifies the volume level at which the Avaya audio brand is played. The options are: • **12db below nominal** • **9db below nominal** • **6db below nominal** • **3db below nominal** • **Nominal (default)** • **3db above nominal** • **6db above nominal** • **9db above nominal**
Phone Mute Alert	Specifies whether the Mute Alert feature is blocked.

Table continues…

Name	Description
	The options are: • **Unblocked** • **Blocked (default)**
Extend Ringtone	Specifies the audio files to customize the ring tone. Value format: the list of file names in `.xml` format separated by commas. The default value is empty.
Group Number	Specifies group numbers if available. The valid value is an integer from 0 to 999. The default value is 0.
Minimum delay to backup volume level to PPM	Specifies the minimal time in seconds between backups of the volume levels to the PPM service when the phone is registered to Avaya Aura® Session Manager. The valid value is an integer from 0 to 900. The default value is 2.
Audio	
Call Progress Tone Country	Specifies the country of operation. The valid value is a sting of 0 to 255 characters. The default value is **USA**.
AGC Handset	Specifies the Automatic Gain Control setting for the handset. The options are: • **Disable** • **Enable (default)**
AGC Headset	Specifies the Automatic Gain Control setting for the headset interface. The options are: • **Disable** • **Enable (default)**
AGC Speaker	Specifies the Automatic Gain Control setting for the speaker. The options are: • **Disable** • **Enable (default)**
Handset Sidetone Level	Specifies the level of side tone in the handset. The options are: • **Normal level (default)**

Table continues…

Name	Description
	• **Three levels softer than Normal** • **Off** • **One level softer than Normal** • **Two levels softer than Normal** • **Four levels softer than Normal** • **Five levels softer than Normal** • **Six levels softer than Normal** • **One level louder than Normal** • **Two levels louder than Normal**
Ringtone Style	Specifies the style of the classic ring tone. The options are: • **North America (default)** • **European**
Handset Profiles	Specifies an ordered list of names to be displayed for handset audio profile selection. The list contains audio profiles set in the web interface, the `46xxsettings.txt` file and internally, for example: `Default,Normal,Amplified,Hearing Aid`. The default value is empty.
Handset Profile Default	Specifies the number of the default handset audio profile. The options are from 1 to 20. The default value is 1.
Dialing	
Dial Plan	Specifies the dial plan used in the phone. Value format: a sting of 0 to 1023 characters without any intervening spaces. 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. The valid value is an integer from 0 to 60. The default value is 20 seconds.
Inter-digit Wait Timer	Specifies the time in seconds during which phone waits after a digit is dialed before sending a `SIP INVITE`. The valid value is an integer from 0 to 10. The default value is 5 seconds.

Table continues…

Name	Description
Dial Local Area Code	Specifies whether the user must dial the area code of calls within the same area code regions. The options are: • **No (default)** • **Yes**
Local Area Code	Indicates the phone local area code which allows the user to dial local numbers with more flexibility. The valid value is a sting of 5 digits ranged from 0 to 9. The default value is empty.
Enhanced Local Dialing Rules	
Enable Local Dialing Rules	Specifies whether the algorithm defined by parameters in this section is used during certain dialing procedures. The options are: • **Disable** • **Enable without Contacts (default)** • **Enable with Contacts**
Country Code	Specifies the country code of the phone. The valid value is an integer from 1 to 999. The default value is 1.
International Access Code	Specifies the international access code. The valid value is up to 4 dialable characters. The default value is 011. Value format: digits from 0 to 9, *, #.
Long Distance Access Code	Specifies the long distance access code. The valid value range is a sting of integers from 0 to 9, and empty. The default value is 1.
Internal Extension Number Length	Specifies the length of an internal extension number. The valid value is an integer from 3 to 13. The default value is 5.
National Telephone Number Length	Specifies the length of a national phone number. The valid value is an integer from 5 to 15. The default value is 10.
Outside Line Access Code	Specifies the number for making an outside call, i.e. a local call in a public network. The valid value is up to 2 dialable characters. The default value is 9. Value format: digits from 0 to 9, *, #.

Table continues…

Name	Description
Remove PSTN access prefix from outgoing number	Allows dialing digits during failover and removing of the PSTN access prefix from the outgoing number. The options are: • **No (default)** • **Yes**
Admin	
Admin Access allowed from Phone	Specifies whether the craft procedures are used for the phone configuration. The options are: • **Yes (default)** • **No**
Admin Login fail attempt allowed	Specifies the number of failed attempts to enter the Administration access code before the login is locked. The options are from 1 to 20. The default value is 10.
Admin Login Locked Time after fail attempt	Specifies the time interval in minutes to re-enter the Administration access code after the login is locked. The valid value is an integer from 5 to 1440. The default value is 10 minutes.
MLPP	
Enable MLPP	Specifies whether the MLPP feature is enabled. The options are: • **Disable (default)** • **Enable**
Maximum Precedence Level	Specifies the maximal allowed precedence level for the user. The options are from 1 to 5. The default value is 1.
MLPP Network Domain	Specifies the MLPP Network Domain. The valid values are: empty, “uc” and “dsn”. The default value is empty.
MLPP Precedence Domain	Specifies the MLPP Precedence Domain. The valid value is a sting of alphanumeric characters. The default value is “000000”.
Enable Precedence Softkey	Controls whether the **Precedence** soft key should be displayed on idle line appearances on the phone screen. The options are: • **Disable** • **Enable (default)**

Table continues…

Name	Description
Guest Login	
Guest Login Enable	Specifies whether the Guest Login feature is available on the phone. The options are: • **Disable (default)** • **Enable**
Guest Login Session Duration (hours)	Specifies the time interval in hours before a guest or a visiting user will be automatically logged off if the telephone is idle. The valid value is an integer from 1 to 12. The default value is 2 hours.
Guest Login Session Warning Time (minutes)	Specifies the time interval in minutes before a warning of the automatic logoff is initially displayed for a guest or a visiting user. The valid value is an integer from 1 to 15. The default value is 5 minutes.
Save Extension	
Show Last Extension	Specifies whether the extension is displayed after logging out. The options are: • **Disable (default)** • **Enable**
Bluetooth	
Bluetooth Enable	Specifies whether Bluetooth can be enabled in the phone menu. The options are: • **Disable** • **Enable (default)**
CCMS	
Media Preservation	Specifies whether a call will be preserved when there is no SIP connectivity to IP Office. This setting is applied only in the Avaya Aura® environment. The options are: • **Disable** • **Enable (default)**
Preserved Call Duration	Specifies the time interval in minutes during which the call is preserved. To apply this setting, **Enable IP Office** should be set to **CCMS** and **Media Preservation** should be enabled.

Table continues…

Name	Description
	Note: This setting is applied only in the Avaya Aura® environment. The valid value is an integer from 10 to 120. The default value is 120 minutes.
Brightness	
Display Brightness	Adjusts the brightness of the phone display. The options are from 1 to 5. The default value is 4.
Button Module #1 Display Brightness	Adjusts the display brightness of the first attached button module. **Note:** If no button modules are attached to the phone, this field is disabled. The options are from 1 to 5. The default value is 4.
Button Module #2 Display Brightness	Adjusts the display brightness of the second attached button module. **Note:** If no button modules are attached to the phone, this field is disabled. The options are from 1 to 5. The default value is 4.
Button Module #3 Display Brightness	Adjusts the display brightness of the third attached button module. **Note:** If no button modules are attached to the phone, this field is disabled. The options are from 1 to 5. The default value is 4.

Related links

Configuring Settings on page 66

Configuring date and time

About this task

Avaya J100 Series IP Phones display the details of the configuration fields in the Description section.

Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **Date & Time**.
3. In the SNTP area, configure the following:
   - **SNTP Server**: Type the SNTP server IP address.
   - **SNTP SYNC Interval**: Type the SNTP synchronization time interval in minutes to re-synchronize the phone's local time . The valid value is from 60 to 2880 minutes. The default synchronization time is 1440 minutes.
   - **GMT Offset**: Type the time between the local standard time and Greenwich Mean Time (GMT) in hours and minutes. The valid value is from 0:00 to ±12:59.
4. 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 adjustments (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.

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

Configuring management settings

About this task

Avaya J100 Series IP Phones display the details of the configuration fields in the Description section.

Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **Management**.
3. Configure the following areas:
   - Device Enrollment Server
   - HTTP Provisioning Server
   - HTTPS Provisioning Server
   - Configuration
   - Firmware
   - Backup/Restore User Data

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

Related links

Management settings field descriptions on page 81

Management settings field descriptions

Name	Description
Device Enrollment Service	
DES Discovery	Specifies the DES Discovery mode. The options are: • **Enable (default)** • **Disable** • **Disable and Restored with Reset to Default**
Embedded Public Certificates	Specifies whether to trust the embedded public certificates. The options are: • **Trusted only if Trustcerts is empty (default)** • **Always Trusted**
HTTP Provisioning Server	
HTTP Server Address	Specifies the IP address of the of the provisioning file server. The valid value is the IP address in the dotted decimal name format, DNS name format or colon-hex. The default value is “0.0.0.0”.
HTTP Server Directory Path	Specifies the path all configurations and data files the device might request when starting up. This path is relative to the root of the HTTP file server, to the directory in which the device configuration and date files are stored. The valid value is a sting of up to 127 ASCII characters without spaces. The default value is empty.
HTTP Port	Specifies the HTTP port address.

Table continues…

Name	Description
	The valid value is an integer from 0 to 65535. The default port number is 80.
HTTPS Provisioning Server	
HTTPS Server Address	Specifies the IP address of the HTTPS provisioning file server. The valid value is the IP address in the dotted decimal name format, DNS name format or colon-hex. The default value is “0.0.0.0”.
HTTPS Server Directory Path	Specifies the path all configurations and data files the device might request when starting up. 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. The valid value is a sting of up to 127 ASCII characters without spaces. The default value is empty.
HTTPS Port	Specifies the HTTPS port address. The valid value is an integer from 0 to 65535. The default is 443.
Configuration	
Configuration Server Access Mode	Specifies the server access mode of the provisioning server. The options are: • **HTTP** • **HTTPS (default)** **Note:** Use HTTPS if the SIP transport mode is TLS, otherwise, use HTTP.
Download configuration file using HTTPS only	Specifies whether only HTTPS is used to download the settings file. The options are: • **Yes** • **No (default)**
Import Configuration File	Enables the user to import the settings file. To import the settings file, click **Browse** to browse your local PC or any PC connected to the network. Select the file and click **Import**.

Table continues…

Name	Description
	Note: Restart the phone for new parameters from the settings file to take effect.
Export Configuration File	Enable user to export a configuration file. To export the configuration file, click **Export** .
Firmware	
Software Version	Displays the version of the SIP software. The default value is empty.
Backup Software Version	Displays the backup software version. The default value is empty.
Firmware Upgrade	Enables the user to import the firmware upgrade file from a local PC or any PC connected to the network. To upload the firmware upgrade file, click **Browse** to browse your PC, select the file and click **Upgrade**. The phone reboots after you select **Yes** in the prompt.
Backup/Restore User Data	
User store Address for Backup/Restore	Specifies the IP address or the DNS name used for HTTP(S) data backup and retrieval. 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.

Related links

Configuring management settings on page 80

Changing the password of the web interface and the phone admin

About this task

Use this procedure to change the administrator password for the phone Administration menu and the web interface.

Your administration password must be between 8 to 31 alphanumeric characters including upper, lower, and special characters. Your password must contain at least 2 digits. You can use special characters such as: tilde (~), exclamation mark (!), at (@), pound (#), dollar ($), percent (%), carat

(^), ampersand (&), asterisk (*), underscore(_), minus (-), plus (+), equal (=), back quote (`), pipe (|), back slash (\), parenthesis (()), braces ({}), brackets ([]), colon (:), semicolon (;), single quote ('), lesser than (<), greater than (>), comma (,), period (.), question mark (?), forward slash (/).

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 **Web Admin Password** section, do the following:
   a. Enter your current password in the **Current Password** field.
   b. Enter your new password in the **New Password** field.
   c. Re-enter your new password in the **Confirm Password** field.
   d. Click **Save**.
4. In the **Phone Administration Menu Password** section, do the following:
   a. Enter your web administrator password in the **Web Administrator Password** field.
   b. Enter your new password in the **New Password** field.
   c. Re-enter your new password in the **Confirm Password** field.
   d. Click **Save**.

Debugging

About this task

Avaya J100 Series IP Phones display the details of the configuration fields in the Description section.

Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **Debugging**.
3. Configure the fields in the following areas:
   - Log
   - SNMP
   - RTCP Monitoring
   - Phone Report
   - SSH
   - SLA Monitor
   - Other

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

Related links

Debugging field descriptions on page 85

Debugging field descriptions

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

Table continues…

Name	Description
	• **Disable (default)**
SNMP	
SNMP String	Specifies the SNMP community name string. The valid value is a string of up to 32 ASCII characters. The default value is empty.
SNMP Address	Specifies the IP addresses for SNMP queries. The valid value is a string of up to 255 ASCII characters without any intervening spaces. The default value is empty.
RTCP Monitoring	
RTCP Monitor Address	Specifies the IP or DNS address of the RTCP monitor. The valid value is a string of up to 255 ASCII characters. The default value is empty.
RTCP Monitor Port	Specifies the RTCP monitor port number. Valid value is an integer from 0 to 65535. The default value is 5005.
RTCP Monitoring Report Period	Specifies the time interval in seconds for sending out RTCP monitoring reports. Valid value is an integer from 5 to 30. The default value is 5 seconds.
Phone Report	
Phone Report Server Address	Specifies the file server address to send the phone report. Click on **Generate Phone Report**. The valid value is a string of up to 255 ASCII characters.
SSH	
SSH Allowed	Specifies whether Secure Shell (SSH) is supported. The options are: • **Enable** • **Disable (default)** • **Configured using local craft procedure**
SSH Idle Timeout	Specifies the time in minutes after which SSH is disabled. The valid value is an integer from 1 to 32767. The default value is 10 minutes.
SSH Banner File	Specifies the file name or the URL for a custom SSH banner file. The valid value is a string of up to 255 ASCII characters. The default value is empty.

Table continues…

Name	Description
EASG site certificates	Specifies the list of EASG site certificates. Support technicians use these certificates to generate EASG responses for SSH login without access to the Avaya network. The valid value is a string of up to 64 ASCII characters. The default value is empty. **Note:** You can add maximum four certificates.
EASG site Authentication Factor code	Specifies the Site Authentication Factor code associated with the EASG site certificate installed. 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 EASG product certificate that a warning message first appears on the phone screen. Valid value is an integer from 90 to 730. The default value is 365.
SLA Monitor	
SLA Monitor Agent	Specifies the status of the SLA Monitor Agent. The options are: • **Enable** • **Disable (default)**
SLA Monitor Server Address	Specifies the IP address of the SLA Monitor server. Valid value is in the dotted decimal name format. The default value is “0.0.0.0:0”.
Packet Capture (sniffing)	Specifies whether the SLA Monitor agent supports packet capture. The options are: • **Disable (default)** • **Enable with payloads removed from RTP packets** • **Enable with payloads included in RTP packets** • **Controlled from Admin Menu**
Device Control	Specifies whether the SLA Monitor agent supports device control. The options are: • **Disable (default)** • **Enable** • **Controlled from Admin Menu**
Device Performance Monitoring	Specifies whether the SLA Monitor agent supports access to phone performance data.

Table continues…

Name	Description
	The options are: • **Enable** • **Disable (default)**
UDP Port for discovery and test messages	Specifies the port used to receive packets from an SLA Monitor server. Valid value is an integer from 6000 to 65535. The default value is 50011.
Other	
Serial Port	Specifies if the port for network traffic is enabled or disabled. The options are: • **Enable** • **Disable (default)**

Related links

Debugging on page 84

Configuring certificates

About this task

Avaya J100 Series IP Phones display the details of the configuration fields in the Description section.

Procedure

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

Related links

Certificates field descriptions on page 89

Certificates field descriptions

Name	Description
Certificates	
Available Trusted Certificate	Displays the file names of available certificates for authentication.
Upload Trusted Certificate	Specifies the trusted certificate used by the phone. You can also browse and upload the certificates from the local PC by clicking **Browse** > **Import**.
Trusted Certificates file to upload	Specifies the name of the certificate file to be uploaded. The valid value is a string os up to 255 ASCII characters. File names must be separated by commas without any intervening spaces. The default value is empty.
Match Identity to trust certificate	Specifies the status of the TLS server identification. The options are: • **Yes (default)** • **No**
Server Certificate re-check hours	Specifies the time interval in hours for rechecking the expiration and revocation status of the certificates used to establish any existing TLS connections. The valid value is an integer from 0 to 32767. The default value is 24 hours.
Warning on number of days before Certificate expiration	Specifies the number of days before the expiration of a certificate that a warning must first appear on the phone screen. The valid value is an integer from 0 to 99. The default value is 60 days.
FQDN IP Mapping	Specifies a FQDN contained in the certificate when an IP address is used to establish the connection. The parameter is a comma-separated list of names or value pairs where the name is an FQDN and the value is an IP address. The valid value is a string of up to 255 characters without any intervening spaces. The default value is empty.
Online Certificate Status Protocol (OCSP)	
Enable OCSP	Specifies the status of OSCP. The options are: • **Disable (default)** • **Enable**

Table continues…

Name	Description
Action on Unknown Revocation Status	Specifies whether a certificate is authenticated when its revocation status cannot be determined. The options are: • **Certificate revocation operation will accept certificates (default)** • **Certificate is considered to be revoked and TLS connection is closed**
Nonce in OCSP Request	Specifies whether a nonce is added to OCSP requests and expected in OCSP responses. The options are: • **Do not add** • **Add (default)**
OCSP Address	Specifies a URI for an OCSP responder. The URI can be an IP address or a host name. The valid value is a string of up to 255 characters without any intervening spaces. The default value is empty.
OCSP Address Preferred	Specifies the preferred OCSP responder URI. The options are: • **Use OCSP address configured first and then OCSP field of AIA extension of the certificate being checked (default)** • **Use OCSP field of AIA extension of the certificate being checked first and then OCSP address configured**
OCSP Trusted Certificates	Specifies the trusted OCSP certificates to be downloaded. It also acts as a separate trusted certificate repository for the OCSP Trusted Responder Model and contains certificates that the OCSP responder can trust. This value is required if the OCSP responder uses a different CA for the server certificate than the root CA. The valid value is a string of up to 255 characters without any intervening spaces. The default value is empty.
OCSP Hash Algorithm	Specifies the hashing algorithm for an OCSP request. value operation. discuss The options are: • **SHA-1 (default)** • **SHA-256**
Use OCSP Caching	Specifies whether OCSP caching is in use.

Table continues…

Name	Description
	The options are: • **Yes (default)** • **No**
OCSP Cache Expiry	Specifies the time interval in minutes for the OCSP cache expiry. The valid value is an integer from 60 to 10080. The default value is 2880 minutes.
SCEP	
SCEP Server	Specifies the URL address of the SCEP server. The valid value is a string of up to 255 ASCII characters without any intervening spaces. The default value is empty.
Common Name	Specifies the common name for the subject in an SCEP certificate request. The valid value is a string of up to 255 ASCII characters without any intervening spaces. The default value is “$SERIALNO”.
Subject	Specifies the part of SUBJECT in an SCEP certificate request that is common for requests from different device. For example, Organizational Unit, Organization, Location, State, and Country. The valid value is a string of up to 255 ASCII characters without any intervening spaces. The default value is empty.
CA Identifier	Specifies the Certificate Authority Identifier. Certificate Authority servers may require a specific CA Identifier string to accept GetCA requests. If the device works with such a Certificate Authority, the CA identifier string can be set through this parameter. The valid value is a string of up to 255 ASCII characters without any intervening spaces. The default value is “CAIdentifier”.
Initiate renewal on % of Validity Interval	Specifies the percentage of the identity certificate’s Validity interval after which renewal procedures will be initiated. If the renewal time interval has elapsed, the phone starts to contact the SCEP server periodically to renew the certificate. The valid value is an integer from 1 to 90. The default value is 90 percent.
Phone behavior on Pending request	Specifies the functioning of the device when performing certificate enrolment. The options are: • **Poll SCEP server periodically in background** • **Wait until a certificate is received or rejected (default)**
SCEP Password	Specifies a challenge password to use with SCEP.

Table continues…

Name	Description
	The valid value is a string of up to 255 ASCII characters without any intervening spaces. The default value is “$SERIALNO”.
PKCS12	
PKCS12 Address	Specifies the IPv4 or IPv6 URL address, or FQDN from where a PKCS#12 file is to be downloaded. The valid value is a string of up to 255 ASCII characters without any intervening spaces. The default value is empty.
PKCS12 Password Retry Count	Specifies the number of attempts allowed for password entry. The valid value is an integer from 0 to 100. The default value is 3 attempts.
Available Identity Certificate	Specifies the trust certificates used as trust points for TLS connections.
Upload Identity Certificate	Displays available trust certificates for the phone. You can also browse and upload the certificates from the local PC by clicking **Browse** > **Import**.
Web Server	
Available Webserver Certificate	Specifies the trust certificates used as trust points for TLS connections. The valid value must be in `.pem` or `.p12` formats.
Upload Custom Webserver Certificate	Specifies the custom certificates to be uploaded. You can also browse and upload the certificates from the local machine by clicking **Browse** > **Import**
Password for Custom Webserver Certificate	Specifies the password to decrypt the uploaded certificate.

Related links

Configuring certificates on page 88

Configuring Environment Settings

About this task

Avaya J100 Series IP Phones display the details of the configuration fields in the Description section.

Procedure

1. Log in to the web interface as an administrator.
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 a third-party call controller as your environment.
   - **3PCC Server Mode**: To set an operation mode in the third-party call control 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

Avaya J100 Series IP Phones display the details of the configuration fields in the Description section.

Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **Background and Screen Saver**.
3. Configure 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.

Related links

Background Image and Screen Saver field description on page 94

Background Image and Screen Saver field description

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

Related links

Configuring Background and Screen Saver of the Phone on page 93

Configuring Calendar of the phone

About this task

Avaya J100 Series IP Phones display the details of the configuration fields in the Description section.

Procedure

1. Log in to the web interface as an administrator.
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.

Related links

Exchange Calendar field description on page 95

Exchange Calendar field description

Name	Description
Exchange Calendar	
Provide Exchange Calendar	Specifies whether the Exchange Calendar menu is available on the phone. The options are: • **Enable** • **Disable (default)**
Exchange User Domain	Specifies the user domain for the Microsoft Exchange Server. The valid value is a string of up to 255 characters. The default value is empty.
Exchange Email Domain	Specifies the email domain for the Microsoft Exchange Server. The valid value is a string of up to 255 characters. The default value is empty.
Exchange Server List	Specifies the list of Microsoft Exchange Server IP or DNS addresses. The valid value must be in the dotted decimal name format or DNS name format without any intervening

Table continues…

Name	Description
	spaces. The maximal value length is 255 characters. The default value is empty.
Exchange Server Secure Mode	Specifies the exchange server mode. The options are: • **HTTP** • **HTTPS (default)**

Related links

Configuring Calendar of the phone on page 95

Restarting your phone through web interface

Procedure

1. Log in to the web interface as an administrator.
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 as an administrator.
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**.

Chapter 5: Configuring servers and VLAN

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 provide the device configuration parameters. The DHCP server also provides the device with the addresses of the SIP controller and file server.
- HTTP or HTTPS file server: To download and save the software distribution package and the settings file.

In a Device Enrollment Services environment, the DHCP server is used to assign IP addresses to the devices. The device receives the file server address from Device Enrollment Services.

Related links

File Server configuration on page 97
DHCP server configuration on page 104

File Server configuration

A file server is an HTTP or an HTTPS server that is required to download and save the software distribution package and the `Settings` file.

On restarting, the phone checks for software updates and `Settings` files on the specified file servers.

You can provide the file server addresses to phones through one of the following methods:

- DHCP
- LLDP
- Administration menu on the phone
- Settings file

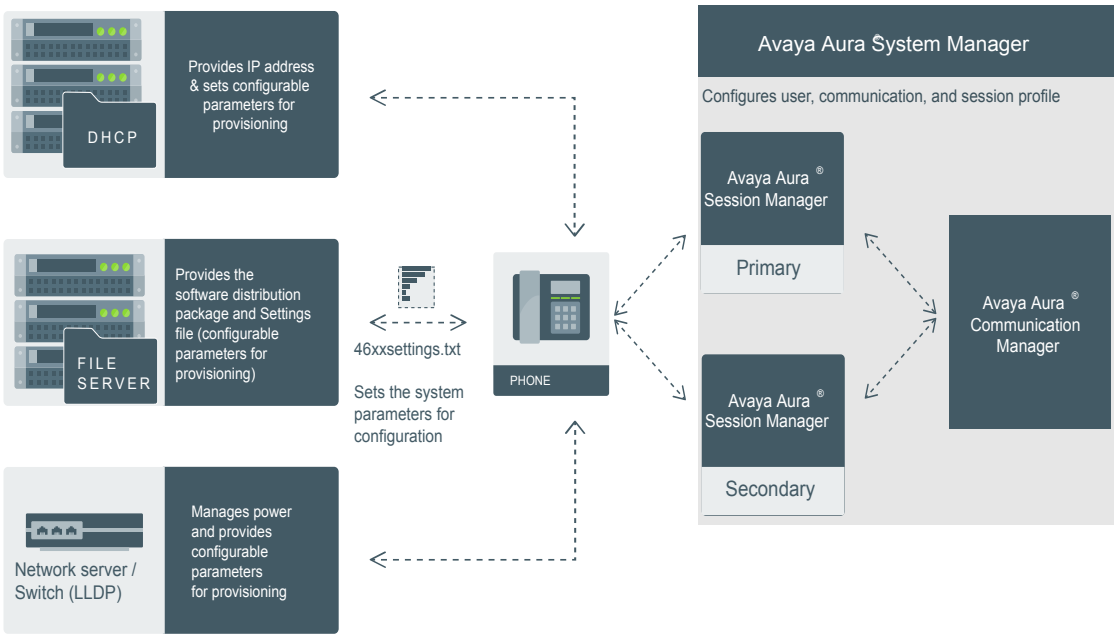


Figure 1: Diagram: Phone setup in Avaya Aura® environment

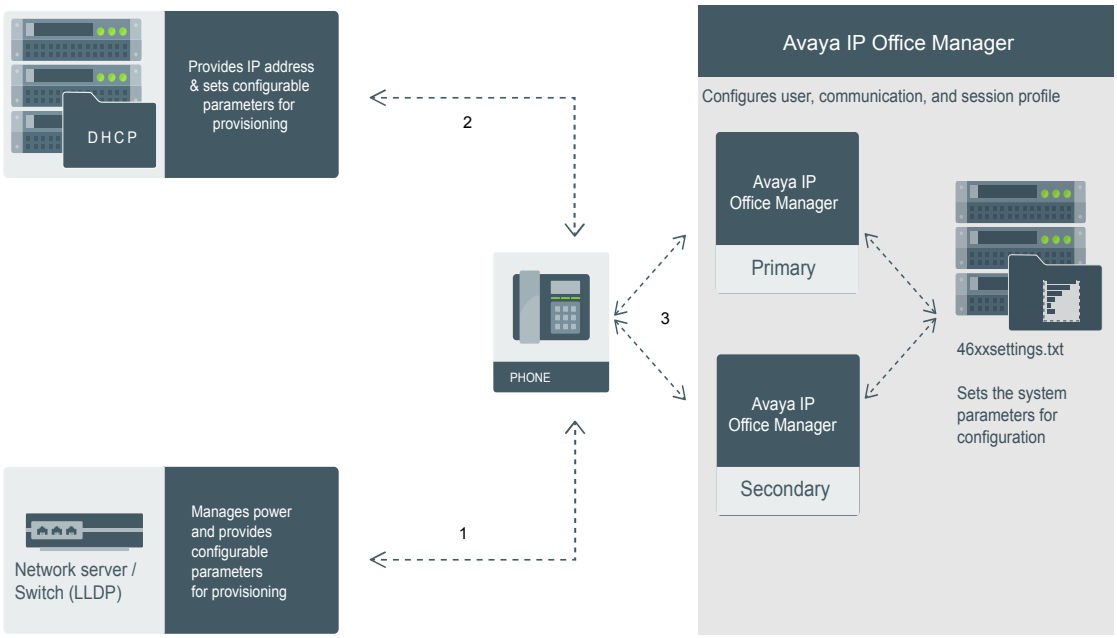


Figure 2: Diagram: Phone setup in IP Office environment

Related links

Server configuration on page 97
Setting up a file server on page 99
Software distribution package on page 100
Downloading and saving the software on page 101
Contents of the settings file on page 101
Modifying the Settings file on page 103

Setting up a file server

About this task

Use this procedure to configure an HTTP or HTTPS file server. You can use the file 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 HTTPS connections, you must initially install a trust certificate through an HTTP server and then transfer to an HTTPS server. Ensure that the TRUSTCERTS parameter includes the root CA certificate of the HTTPS file server identity certificate.

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

Related links

File Server configuration on page 97

Software distribution package

Note:

For any new software release, ensure that you download the latest software distribution package and read any Product Support Notices (PSNs) associated with the new release. Both are 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. To do this, clear the browser cache before downloading the `Settings` file from the Avaya support Web site, so that you don't get an old version.

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

Note:

From IP Office R 10.0 SP3 or later, the software distribution package for the Avaya J100 Series IP Phones is part of the IP Office admin CD.

SIP software distribution package contains:

- One or more software files
- One upgrade file (`J100Supgrade.txt`)
- Language files. For example, `Mlf_J129_BrazilianPortuguese.xml`, `Mlf_J129_Chinese.xml`.
- Files av_prca_pem_2033.txt and av_sipca_pem_2027.txt that contain a copy of the Avaya Product Root Certificate Authority certificate in PEM format that may be downloaded to phones based on the value of the TRUSTCERTS parameter.
- File named release.xml that is used by the Avaya Software Update Manager application. Avaya Software Update Manager upgrades and maintains firmware for Avaya managed devices.

Note:

Settings files are not included in the software distribution packages because they would overwrite your existing files and settings.

Two configuration files that are important to understand are as follows:

- The upgrade file, `J100Supgrade.txt` that tells the phone whether the phone needs to upgrade software. The phones attempt to read this file whenever they reset. The upgrade file is also used to point to the `Settings` file.

- The Settings file, `46xxsettings.txt`, that contains the option settings that enable, disable, or otherwise customize the settings you might need to tailor the phones for your enterprise. IP Office auto generates the Settings file (`J100settings.txt`).

Related links

File Server configuration on page 97

Downloading and saving the software

Before you begin

Ensure that your file 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 file server.
7. Extract the zipped file and save it at an appropriate location on the file 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 file server.

Related links

File Server configuration on page 97

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.
- Conditionals, of the form **IF *$parameter_name* SEQ *string* GOTO *tag***. Conditionals cause the **Goto** command to be processed if the value of the parameter named ***parameter_name*** exactly matches ***string***. If no such parameter named ***parameter_name*** exists, the entire conditional is ignored. The only parameters that can be used in a conditional statement are: GROUP, MACADDR, MODEL and MODEL4.

- **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.

The Avaya-provided upgrade file includes a line that tells the phones to **GET *46xxsettings.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 Web site.

During a reboot, if the phone is unable to access the settings file, it does not retain the values of all the parameters. For more information on which parameter value is retained, see the following table.

Parameter	Retained
AGCHAND	Y
AGCHEAD	Y
AGCSPKR	Y
APPNAME	N
AUDIOENV	N
AUDIOSTHD	N
AUDIOSTHS	N
AUTH	Y
BAKLIGHTOFF	Y
CNGLABEL	Y
DAYLIGHT_SAVING_SET TING_MODE	Y
DHCPSTD	N
HEADSYS	N
HOMEIDLETIME	N
LOG_CATEGORY	Y
LOGSRVR	N
LOCAL_LOG_LEVEL	Y

Table continues…

Parameter	Retained
LANG0STAT	Y
MSGNUM	N
PROCSTAT	Y
PROCPSWD	Y
PHY1STAT	Y
PHY2STAT	Y
PHNCC	N
PHNDPLENGTH	N
PHNIC	N
PHNLDLENGTH	N
PHNLD	N
PHNLAC	Y
PHNOL	N
RFSNAME	N
SNMPADD	Y
SNMPSTRING	Y
SIG	Y
SCREENSAVERON	N
TEAM_BUTTON_RING_T YPE	Y
TPSLIST	N
VLANTEST	Y

Related links

File Server configuration on page 97

Modifying the Settings file

About this task

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

Note:

This procedure applies to Avaya Aura® environment only. In IP Office, the settings file is autogenerated and cannot be modified.

Procedure

1. On the file server, go to the directory of the `Settings` file.
2. Open the `Settings` file in a text editor.

3. Set the values of the parameters that you want to provision.
4. Save the `Settings` file.

Result

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

Related links

File Server configuration on page 97
List of configuration parameters on page 194

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 receives the file server address from the DES server.

Related links

Server configuration on page 97
Setting up a DHCP server on page 104

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 104

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 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 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.

Table continues…

Category	TLV Name (Type)	TLV Info String (Value)
Basic Optional	System Capabilities	Bit 2 (Bridge) will be set in the System Capabilities if the phone has an internal Ethernet switch. If Bit 2 is set in Enabled Capabilities then the secondary port is enabled.
Basic Optional	Management Address	Mgmt IPv4 IP address of device. Interface number subtype = 3 (system port). Interface number = 1. OID = SNMP MIB-II sysObjectID of the device.
IEEE 802.3 Organization Specific	MAC / PHY Configuration / Status	Reports auto negotiation status and speed of the uplink port on the device.
TIA LLDP MED	LLDP-MED Capabilities	Media Endpoint Discovery capabilities = 00-33 (Inventory, Power-via-MDI, Network Policy, MED Caps).
TIA LLDP MED	Network Policy	Tagging Yes/No, VLAN ID for voice, L2 Priority, DSCP Value.
TIA LLDP MED	Inventory – Hardware Revision	MODEL - Full Model Name.
TIA LLDP MED	Inventory – Firmware Revision	Firmware version.
TIA LLDP MED	Inventory – Software Revision	Software version or filename.
TIA LLDP MED	Inventory – Serial Number	Device serial number.
TIA LLDP MED	Inventory – Manufacturer Name	Avaya.
TIA LLDP MED	Inventory – Model Name	MODEL with the final Dxxx characters removed.
Avaya Proprietary	Call Server IP address	Call Server IP Address. Subtype = 3.
Avaya Proprietary	IP Phone addresses	Phone IP address, Phone Address Mask, Gateway IP Address. Subtype = 4.
Avaya Proprietary	File Server	File Server IP Address. Subtype = 6.
Avaya Proprietary	802.1Q Framing	802.1Q Framing = 1 if tagging or 2 if not.
Basic Mandatory	End-of-LLDPDU	Not applicable.

TLV impact on system parameter values

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

Table continues…

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

Configuration through DHCP

The 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 .
- 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.
```

Following parameters can be configured with this feature:

Parameter	Description
ADMIN_PASSWORD	Specifies the security string used to access local procedures. The default is 27238. This is meant to replace PROCPSWD as it provides a more secure password syntax.
HTTPDIR	Specifies the path to prepend to all configurations and data files the device might request when starting up, that is, the path, relative to the root of the HTTP file server, to the directory in which the device configuration and date files are stored. The path may contain no more than 127 characters and may contain no spaces. HTTPDIR is the path for all HTTP operations. The command is `SET HTTPDIR=<path>`. In configurations where the upgrade and binary files are in the default directory on the HTTP server, do not use the `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. 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

Table continues…

Parameter	Description
	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. The default is 27238. ADMIN_PASSWORD replaces this parameter if ADMIN_PASSWORD is set in the `46xxsettings.txt` file.
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.
TLSDIR	Used as path name that is prepended to all file names used in HTTPS GET operations during initialization. The string length can be from 0 to 127.
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. **Note:** 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 autogenerated. 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.

Table continues…

Option	Description
Option 3	Specifies the gateway IP address list. The list can contain up to 127 total ASCII characters. Separate more than one IP address with commas with no intervening spaces.
Option 6	Specifies the DNS server address list. The list can contain up to 127 total ASCII characters. Separate more than one IP address with commas with no intervening spaces. The phone supports DNS and the dotted decimal addresses. The phone attempts to resolve a non-ASCII-encoded dotted decimal IP address by checking the contents of DHCP Option 6. At least one address in option 6 must be a valid, nonzero, dotted decimal address, otherwise the DNS address fails.
Option 12	Specifies the host name. `AVohhhhhh`, where: • `AV` stands for Avaya. • `o` is one of the following values based on Object Unique Identifier (OUI) derived from the first three octets of the phone MAC address: - A if OUI is 00-04-0D - B if OUI is 00-1B-4F - E if OUI is 00-09-6E - L if OUI is 00-60-1D - T if the OUI is 00-07-3B - X if the OUI is anything else • `hhhhhh` are the ASCII characters for the hexadecimal representation of the last three octets of the phone MAC address.
Option 15	Specifies the domain name. The domain name is required to resolve DNS names into IP addresses. Configure this option if you use a DNS name for the HTTP server. Otherwise, you can specify a domain as part of customizing the HTTP server. This domain name is appended to the DNS addresses specified in option 6 before the phone attempts to resolve the DNS address. The phone queries the DNS address in the order they are specified in option 6. If there is no response from an address, the phone queries the next DNS address. As an alternative to administering DNS by DHCP, you can specify the DNS server and domain name in the HTTP script file. If you use the script file, you must configure the DNSSRVR and DOMAIN parameters so that you can use the values of these parameters in the script. **Note:** Administer option 6 and option 15 appropriately with DNS servers and domain names respectively.

Table continues…

Option	Description
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.
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 sname and file parameters.
Option 53	Specifies the DHCP message type. The value can be one of the following: • 1 for DHCPDISCOVER • 3 for DHCPREQUEST For DHCPREQUEST sent to renew the device IP address lease: • If a DHCPACK is received in response, a log event record is generated with a Log Category of DHCP. • If a DHCPNAK is received in response, the device immediately ceases IP address usage, generates a log event record, sets IPADD to 0.0.0.0, and enters the DHCP INIT state.
Option 55	Specifies the parameter request list. Acceptable values are: • 1 for subnet mask • 3 for router IP addresses • 6 for domain name server IP addresses • 7 for log server • 15 for domain name • 42 for NTP servers
Option 57	Specifies the maximum DHCP message size. Set the value to 1500. Set the value to 1000.
Option 58	Specifies the DHCP lease renew time. If not received or if this value is greater than that for option 51, the default value of T1, renewal timer is used.
Option 59	Specifies the DHCP lease rebind time. If not received or if this value is greater than that for Option 51, the default value of T2, rebinding timer is used.

Table continues…

Option	Description
Option 242	Specifies the site-specific option. This option is optional. If you do not configure this option, ensure that one of the following parameters is configured appropriately elsewhere: • HTTPSRVR • TLSSRVR

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

support configuration of network parameters to the phone using DHCP as per RFC 2131. However, when a DHCP server becomes unreachable and the DHCP lease currently held by the phone expires, the phones continues to use the same lease until the DHCP server becomes reachable. This feature is controlled with the help of configuration parameter, DHCPSTD, as explained:

Parameter name	Default value	Description
DHCPSTD	0	Specifies it will continue to use the expired DHCP lease. Value operation: • 0: Continue use of expired DHCP lease if the lease could not be renewed.

Parameter name	Default value	Description
		• 1: Stop using DHCP lease immediately when it expires, as per standard. The parameter is configured through `46xxsettings.txt` file.

When this feature is enabled (DHCPSTD=1), the phone will continue 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 continue attempting to reach a DHCP server every 60 seconds. When a DHCP server becomes reachable 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

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 might 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

Virtual LAN (VLAN) overview

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.

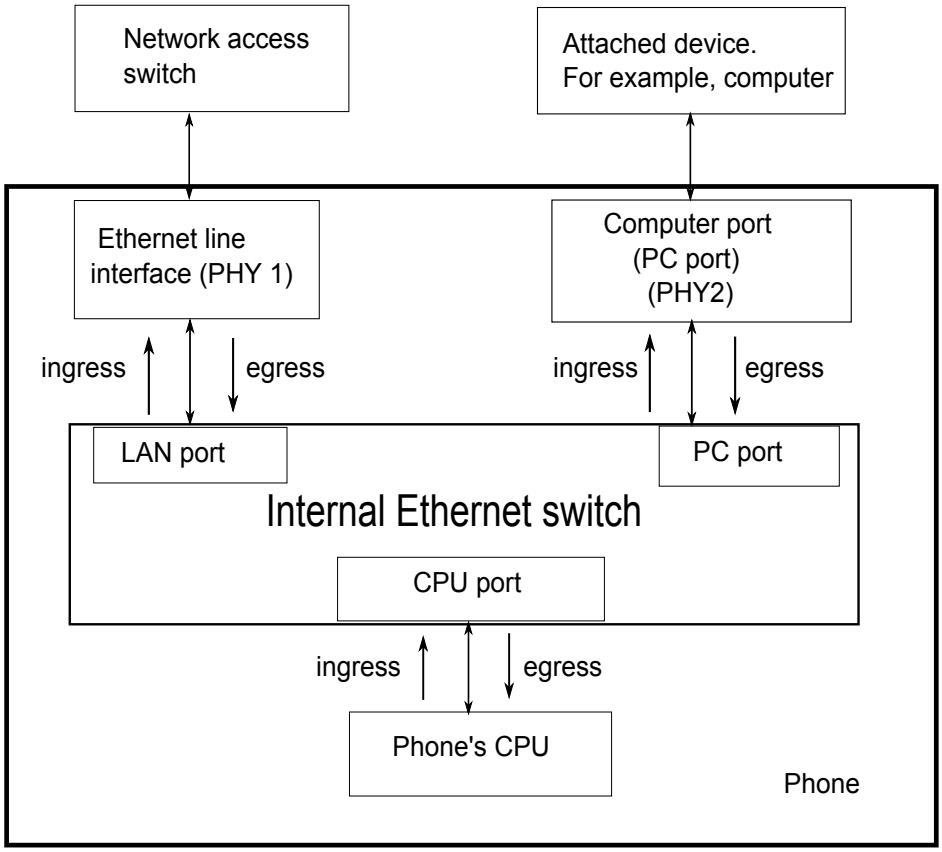
Related links

VLAN separation on page 115
External switch configuration on page 117
Exceptions to the VLAN forwarding rules on page 118
Special considerations on page 118
VLAN parameters on page 119

VLAN separation

The Avaya J100 Series IP Phones has 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 the data destined to the PC port.

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.


Network access switch
Attached device. For example, computer
Ethernet line interface (PHY 1)
Computer port (PC port) (PHY2)
ingress
egress
ingress
egress
LAN port
PC port
Internal Ethernet switch
CPU port
ingress
egress
Phone's CPU
Phone

Related links

Virtual LAN (VLAN) overview on page 114
VLAN separation modes on page 117

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 frames 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 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
  - The phone actually sends tagged VLAN frames. This means that the DHCP server on voice VLAN (L2QVLAN) is reachable and the phone receives IP address on voice VLAN.

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 115

External switch configuration

Configure the following for the external switch port:

- Bind VLAN to the voice VLAN (L2QVLAN) and the data VLAN (PHY2VLAN). It is important to restrict the VLAN binding when in No VLAN separation mode. This is because there is no filtering by the internal phone switch and the CPU of the phone is subject to all the traffic

going through the phone. When in Full VLAN separation mode, the internal phone switch will filter any tagged VLAN frames with VLANs other than voice VLAN (L2QVLAN) and data VLAN (PHY2VLAN) in any case. However, you must configure only the necessary VLANs on the external switch port.

- Set the default VLAN as the data VLAN (PHY2VLAN). This is the VLAN assigned by the external switch port to untagged frames received from phone LAN port.
- 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.

Sending egress voice VLAN frames untagged from the external switch port to the phone LAN port means that there is no VLAN separation between the voice VLAN and data VLAN.

Related links

Virtual LAN (VLAN) overview on page 114

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) overview on page 114

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 the VLAN functionality of the phone is set to one of the following:

- L2Q=1: With a VLANID =0
- L2Q=0: Without any VLAN tag

The VLANTEST parameter determines how long the phone waits for a recognizable DHCPOFFER. If VLANTEST= 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 on VLANs that are not equal to L2QVLAN.

Related links

Virtual LAN (VLAN) overview on page 114

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 the VLAN tagging is enabled or disabled. Value operation: • 0: Auto. VLAN tagging is turned on when the network can support VLAN tagging and L2QVLAN is non zero. • 1: On. VLAN tagging is turned on when the network can support VLAN tagging. The IP phone sends tagged frames with VLAN = L2QVLAN, even if L2QVLAN is set to 0. • 2: Off. VLAN functionality is disabled. L2Q is configured through: • Local admin procedure • A name equal to value pair in DHCPACK message • SET command in the `Settings` file

Table continues…

Parameter name	Default value	Description
		• DHCP option 43 • LLDP
VLANTEST	60	Specifies the number of seconds that the phone waits prior to failing back to a different VLAN ID if no response is received from the DHCP server. Valid values are 0 through 999. Value operation: • 0: The phone continues to attempt a DHCP REQUEST forever. VLANTEST is configured through: • `Settings` file • A name equal to value pair in DHCPACK message
VLANSEP	1	Specifies whether the VLAN separation is enabled or disabled by the built-in Ethernet switch. Value operation: • 0: Disabled • 1: Enabled
VLANSEPMODE	1	Specifies whether the VLAN separation is enabled or disabled. Value operation: • 0: Disabled • 1: Enabled VLANSEPMODE is configured through the `Settings` file.
PHY2TAGS	0	Determines whether or not VLAN tags are stripped on Ethernet frames going out of the Computer (PC) port. Value operation: • 0: Strip tags. VLAN tags are stripped from Ethernet frames leaving the computer (PC) port of the phone. • 1: Does not strip tags. VLAN tags are not stripped from Ethernet frames leaving the Computer (PC) port of the phone.

Table continues…

Parameter name	Default value	Description
		PHY2TAGS is configured through the `Settings` file.
L2QVLAN	0	Specifies the voice VLAN ID to be used by IP phones. Valid values are 0 through 4094. L2QVLAN is configured through: • Local admin procedure • A name equal to value pair in DHCPACK message • SET command in the `Settings` file • DHCP option 43 • LLDP
PHY2VLAN	0	Specifies the value of the 802.1Q VLAN ID that is used to identify network traffic going into and coming out of the internal CPU of the phone. Valid values are 0 through 4094. PHY2VLAN is configured through: • SET command in the `Settings` file • LLDP
L2QAUD	6	Specifies the value of the VLAN priority portion of the VLAN tag when the phone generates tagged Ethernet frames from the internal CPU of the phone. These values are inserted into the VLAN tag for audio frames (RTP, RTCP, SRTP, SRTCP). All other frames except those specified by the L2QSIG parameter are set to priority 0. Valid values are 0 through 7. L2QAUD is configured through: • SET command in the `Settings` file • LLDP
L2QSIG	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 signaling frames (SIP). All other frames except those specified by the L2QAUD parameter are set to priority 0. Valid values are 0 through 7.

Table continues…

Parameter name	Default value	Description
		L2QSIG is configured through: • SET command in the `Settings` file • LLDP

Related links

Virtual LAN (VLAN) overview on page 114

IPv4 and IPv6 overview

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 125.

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 124.

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 adresses.

Note:

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

Before you begin

Obtain the access code to Administration menu.

Procedure

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

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

Configuring IPv4 from the web interface

Before you begin

Obtain the access code to Administration menu.

On the phone, use Administration menu for the following:

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

See Enabling access to the web interface through the Phone Administration menu on page 41 and Viewing IP address of the phone on page 42 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 and logging out of the web interface on page 43.
3. Navigate to **Ethernet** > **IPv4 Configuration**.
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 3155 standard and immediately stop using an IPv6 address if the address valid lifetime expires, or whether it will enter an extended rebinding state. Value operation: • 0: DHCPv6 enters proprietary extended rebinding state (continue to use IPv6 address, if DHCPv6 lease expires). • 1: DHCPv6 complies with IETF RFC 3155 standard (immediately release IPv6 address, if DHCPv6 lease expires).
DUAL_IPPREF	4	DUAL_IPPREF controls the following: • The selection of SSON either from DHCPv4 or DHCPv6 server, when phone is in dual mode, and

Table continues…

Parameter name	Default value	Description
		• Whether an IPv4 or IPv6 addresses returned by DNS would be tried first during dual-mode operation. DHCP clients use DUAL_IPPREF to decide which SSON configuration attributes to apply for DHCPv4/DHCPv6 interworking in dual mode. Value operation: • 4(Default): IPv4 is preferred. • 6: IPv6 is preferred.
PRIVACY_SLAAC_MODE	1	Specifies the preference for Privacy Extensions. Value operation: • 0: Disable Privacy Extensions. • 1(Default): Enable Privacy Extensions, and prefer public addresses to temporary addresses. • 2: Enable Privacy Extensions, and prefer temporary addresses to public addresses.
IPV6STAT	1	Specifies the mode of the IP family which will be used in the current configuration. Value operation: • 0: Only IPv4 mode is enabled. • 1(Default): Dual mode is enabled. • 2: Only IPv6 mode is enabled.

Configuring IPv6 from the phone menu

About this task

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

Note:

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

Before you begin

Obtain the access code to Administration menu.

Procedure

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

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

Configuring IPv6 from the web interface

Before you begin

Obtain the access code to Administration menu.

On the phone, use Administration menu for the following:

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

See Enabling access to the web interface through the Phone Administration menu on page 41 and Viewing IP address of the phone on page 42 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 and logging out of the web interface on page 43.

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

IPv6 limitations

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

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 a single user.

With MDA, you 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.

  You can alert other registered devices about an incoming call to your extension. When you answer 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, you 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 you bridge on to a call on the registered devices and start a transfer, the call drops from all devices after the transfer is complete.

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

Related links

Shared control on page 129

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. Valid values are 0 to 255 characters in the dotted decimal or colon-hex format. The syntax is: `host[:port][;transport=xxx]` where • `host` is IP addresses in dotted-decimal format or hex format. • `[:port]` is the port number. The default values are 5060 for TCP and 5061 for TLS. • `[;transport=xxx]` is the transport type and `xxx` is either TLS or TCP. The default value is TLS. For example, `SIP_CONTROLLER_LIST_2="10.16.26.88:5060;transport=tcp"`

Table continues…

Parameter	Description
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. Valid values are: • 4: IPv4. This is the default value. • 6: IPv6

Shared control

With the shared control feature. the phones can be controlled from a soft phone client. The phone needs to be registered before establishing a shared control connection. To operate shared control, the value of SIP_CONTROLLER_LIST must be identical for the phone and the soft client. Depending on soft client implementation, a shared control session may not be established if multiple devices are registered to the same user at the same time, with the **`sc-enabled`** flag sent during registration.

Note:

- SIP signaling must be set to TLS for the phone and the soft client. For security reasons, TCP Signaling with shared control is not supported.
- The Avaya J139 IP Phone does not support Shared control feature.

Related links

Multiple Device Access on page 127

Microsoft Exchange Server integration

To integrate with Microsoft® Exchange Server, you need to configure the parameters in the `46xxsettings.txt` file and set the required values in the Settings menu on the phone.

For more information about configuring the parameters via the phone menu, see the “Configuring Microsoft® Exchange Server calendar” section in the using guide of the required phone model.

Configuring the settings file parameters

Set the following parameters in the `46xxsettings.txt` file to specify your company email domain, your company email user domain, and add trust certificates if required:

Parameter name	Default value	Description
MAX_TRUSTCERTS	6	Specifies the maximum number of trusted certificates defined by the TRUSTCERTS parameter which can be downloaded to the phone. Valid values are from 1 to 10. **Note:** Each trusted certificate file may contain more than one certificate.
EXCHANGE_SERVER_LIST	Null	Specifies a list of one or more Exchange server IP addresses. The value can contain up to 255 characters. Addresses can be in dotted-decimal or DNS name format, separated by commas without any intervening spaces.
EXCHANGE_SERVER_SECURE_MODE	1	Specifies whether to use HTTPS to contact Exchange servers. Value Operation: • 0: HTTP is used. • 1: HTTPS is used.
EXCHANGE_EMAIL_DOMAIN	Null	Specifies the Exchange email domain. The value can contain from 0 to 255 characters.
EXCHANGE_USER_DOMAIN	Null	Specifies the Exchange email user domain. The value can contain from 0 to 255 characters.
EXCHANGE_AUTH_USERNAME_FORMAT	0	Specifies the format of the username for user authentication. Value Operation: • 0: Office 2003 / Office2016 username format, for example: `EXCHANGE_USER_DOMAIN \Exchange Username`. • 1: Office 365 username format, for example: `Exchange`

Table continues…

Parameter name	Default value	Description
		`Username@EXCHANGE_USER_DOMAIN`.
TRUSTCERTS	Null	Specifies the list of file names that contain copies of CA certificates (in PEM format) that are downloaded, saved in non-volatile memory, and used by the telephone to authenticate received identity certificates. The value can contain up to 255 characters. The file names should be separated by commas without intervening spaces, for example: `digicertroot.txt,digicertglobalCA.txt,ITserverCA.txt`

Chapter 6: 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 *Avaya IP Office™ Platform 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
Message Waiting Indication	MWI is not available. If the PSTN_VM_NUM parameter is	Yes

Table continues…

Feature	Survivable operation with third-party proxy	Normal operation with Communication Manager and Session Manager
	administered, users can gain to the voice mailbox.	
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

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** softkey on the Login screen, or the Phone screen, or when the user presses the **Yes** softkey 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. 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.

You can set up to 100 emergency numbers for the phones to dial. However, you must first configure the additional emergency numbers in System Manager. You can then use the parameter PHNMOREEMERGNUMS to specify these additional emergency numbers in the `46xxsettings.txt file` or in the Avaya Aura® System Manager.

Note:

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

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** softkey 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** softkey.

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 or not the SIP proxy supports emergency dialing, it is possible to enable this functionality in the overall SIP solution.

Avaya J100 Series IP Phones displays an **Emerg** softkey when the phone is not registered or when the phone is locked. When the **Emerg** softkey 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** sofkey 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 softkey when the phone is registered and whether the phone displays a confirmation dialogue box when **Emerg** softkey is pressed.
- ENABLE_SHOW_EMERG_SK_UNREG: Specifies whether the phone displays Emerg softkey when the phone is not registered and whether the phone displays a confirmation dialogue box when **Emerg** softkey is pressed.

In Avaya J100 Series IP Phones you can set up to 100 additional emergency numbers to dial. You can define the numbers using the following parameter:

- PHNMOREEMERGNUMS: Specifies the additional emergency phone numbers.

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.

Note:

- When in failover, the Emergency Number must be provisioned on the SIP gateway or the user will not be able to dial it.
- 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** softkey 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** softkey.
- 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** soktkey on the phone. User has to manually dial the emergency number.

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*

About 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.

Chapter 7: Security

Security overview

Avaya J100 Series IP Phones provide several updated security features. For example:

SIP-based Avaya J100 Series IP Phones provides several updated security features. When the phone is in a locked state, a user can only receive calls or make emergency calls. User logs and data are protected with the user account.

The following security features are available:

- Account management: The phone supports the following:
  - 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 both private key and certificate.
- Certificate management: The phone supports the following:
  - X509v3 compliant certificates
  - Public Key Infrastructure (PKI) for users who use third-party certificates for all Avaya services including database
  - 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 SSH fingerprint in the Administration menu.
- Display of OpenSSH and OpenSSL version in the Administration menu.
- Display of OpenSSH and OpenSSL version 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 (256 bit symmetric and RSA 2048 and 4096 bit asymmetric keys) 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 certain 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.

Access control and security

Phones provide the following security features for control and access:

Security event logging

Logs are maintained for the following events:

- Successful and failed logins, username lockouts, and registration and authorization attempts by users and administrators.
- Change in roles.
- Firewall configuration changes.
- Modification or access to critical data, applications, and files.

Private Key storage

The phone stores the private key in PKCS#12 and PEM file formats. The phone sends the device identity certificate and a private key along with the encrypted password to the WPA supplicant. EAP-MD5 password is sent 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.

The parameter PROVIDE_NETWORKINFO_SCREEN controls the display of this information.

OpenSSH/OpenSSL version

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

SSH Fingerprint

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

Time synchronization

The phone synchronizes the time with the configured NTP servers 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

Certificate management

Certificates are used to establish secure communication between network entities. Server or mutual authentication can be used to establish a secure connection between a client and server. The client always validates the certificate of the server 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 identity certificate must be provided and validated by the server to establish mutual authentication. 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.

Enhancements for installing identity certificates:

- SCEP over HTTPS is supported for enrollment.

- PKCS#12 file format is supported for installation.

To check the number of days remaining for Identity certificate expiry, use the parameter CERT_WARNING_DAYS . The user is notified through a log message if the log level is maintained as WARNING with the category CERTMGMT. The logs are maintained and displayed if SYSLOG is enabled.

MIB object tables and IDs are created for certificates installed on the phone. You can view the certificate attributes through an SNMP MIB browser.

To implement DES, the phone has 64 Public CA certificates built in. For a list of the certificates, see Appendix B.

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. The following MIB OIDs can be used for this query:

Attribute Name	MIB OID
Serial Number	endptIdentityCertSN
Subject	endptIdentityCertSubjectName
Issuer	endptIdentityCertIssuerName
Validity	endptIdentityCertValidityPeriod
Thumbprint	endptIdentityCertFingerprint
Subject Alt Name	endptIdentityCertSubjectAlternativeName
Key Usage Extension	endptIdentityCertKeyUsageExtensions
Extended Key Usage	endptIdentityCertExtendedKeyUsage
Basic Constraints	endptIdentityCertBasicContraints

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 . The options are: • 0: Identity matching is not performed. • 1: The certificate is trusted only if the identity used to connect to the server matches the certificate identity, as per Section 3.1 of RFC 2818. For SIP-TLS connections, an additional check is performed to validate the SIP domain identified in the certificate, as per RFC 5922. The parameter is configured through the `46xxsettings.txt`.

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 adress. 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.

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.

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.

OCSP trust certificates

Online Certificate Status Protocol (OCSP) is used to check the certificate revocation status of an x509 certificate in use. The phone trusts the OCSP server and installs its CA certificates. 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.

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.
SSH_ALLOWED	0	To keep SSH disabled.

SCEP parameters

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

The SCEP parameters are not supported in IP Office environment.

Parameter	Type	Default value	Description
MYCERTURL	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.
MYCERTCN	String	$SERIALNO	Specifies the Common name (CN) for SUBJECT in SCEP certificate request. The values can either be $SERIALNO or $MACADDR. If the value includes the string $SERIALNO, that string will be replaced by the phones serial number. If the value includes the string $MACADDR, that string will be replaced by the phones MAC address.
MYCERTDN	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.
MYCERTKEYLEN	Numeric	2048	Specifies the private key length in bits to be created in the device for a certificate enrollment. The range is from 1024 to 2048.
MYCERTRENEW	Numeric	90	Specifies the percentage used to calculate the renewal time interval out of the device certificate's Validity Object.

Table continues…

Parameter	Type	Default value	Description
			If the renewal time interval has elapsed the phone starts to periodically contact the SCEP server again to renew the certificate. The range is from 1 to 99.
MYCERTWAIT	Numeric	1	Specifies the behavior of the device when performing certificate enrolment. assign one of the following values: • 0: Periodical check in the background • 1: Wait until a certificate or a denial is received or a pending notification is received
MYCERTCAID	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.
SCEPPASSWORD	String	$SERIALNO	Specifies a challenge password to use with SCEP. The value of SCEPPASSWORD, if non-null, is included in a challengePassword attribute in SCEP certificate signing requests. If the value contains $SERIALNO, $SERIALNO is replaced by the value of SERIALNO. If the value contains $MACADDR, $MACADDR is replaced by the value of MACADDR without the colon separators.

Chapter 8: Phone administration and configuration

Accessing the Admin menu during phone startup

Before you begin

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

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

Procedure

1. Press **Main Menu** softkey.
2. On the Access code screen, enter the admin menu password using the dialpad.
3. Press **Enter**.

Parameters for managing Admin menu

Parameter name	Default value	Description
PROCSTAT	0	Specifies whether Admin menu is used for device configuration. Value operation: • 0: Specifies that the phone is administered through Admin menu. • 1: Specifies that the phone is not administered through Admin menu.
PROCPSWD	27238	Specifies an authentication code for accessing Admin menu. Value operation: • 27238: Specifies that the authentication code `27238` is set for accessing Admin menu.

Table continues…

Parameter name	Default value	Description
		• ASCII numbers between 0–7: Specifies an administrator configured authentication code. You must provide at least four ASCII numbers. • Null: Specifies that no authentication code is required to access Admin menu.
ADMIN_PASSWORD	27238	Specifies an authentication code for accessing Admin menu. When the parameter ADMIN_PASSWORD is set, then the parameter PROCPSWD is not used. You must provide an authentication code by using the any of the following combinations: • Numeric (0–9) • Alphabet in upper case (A-Z) • Alphabet in lower case (a-z) • Special characters **Note:** • PROCPSWD supports only numeric values. ADMIN_PASSWORD supports both alphanumeric and special characters. Hence, for enhanced security, use ADMIN_PASSWORD instead of PROCPSWD. • You can set the PROCPSWD and the ADMIN_PASSWORD in either `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 to 20.
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 to 1440 minutes.

Accessing the Admin menu after log in

Procedure

1. Navigate to **Main Menu** > **Administration**.

2. In the **Access code** field, enter the administration password.

   The default access code is `27238`.

3. Press **Enter**.

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** > **Ethernet IPv4**.

   The phone displays the parameters for IP configuration.

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. Select one of the following: • **YES**: Selects the DHCP option to view the IP addresses. • **No**: Selects the DHCP option to enter the IP addresss.
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 VLAN menu:	
802.1Q	Choose one of the following options: • **Auto**: Automatic mode. • **On**: Turns on the configuration.

Table continues…

Configuration Parameter Name	Description
	• **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 Servers menu:	
HTTP server	Specifies the IP address of the HTTP file server. The available format is `nnn.nnn.nnn.nnn`.
HTTPS server	Specifies the IP address of the HTTPS file server. The available format is `nnn.nnn.nnn.nnn`.
DNS server	Specifies the IP address of the DNS server. The available format is `nnn.nnn.nnn.nnn`.
SNTP server	Specifies the time server settings.
The following parameters are available in Auto provisioning menu:	
Service	Specifies option for auto provisioning. Press **Toggle** to choose the required option : • **Inactive** • **Active**
Certificate	Specifies if the certificate is available.
Certificate Expiry	Specifies the expiry date of the certificate. The available format is `DD-MMM-YYYY`

Using the debug mode

About this task

Use this procedure to activate or deactivate the debugging options.

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**.

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 interface**.
5. Use the **Right Arrow** key to change **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 **Change** softkey 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 **Change** softkey to change the PC Ethernet setting to one of the following:
   - **Auto**
   - **10Mbps half**
   - **10Mbps full**
   - **100Mbps half**
   - **100Mbps full**
   - **Disabled**
8. Press **Save**.

Group identifier

A group identifier is a number assigned to a particular community of IP phone users in an organization. The group identifier number can be a number from 0 to 999 and the default number is 0.

With a group identifier, you can provide administration settings to each phone used by different communities of end users. For example, you might want to group users by time zones or work activities.

You can configure group identifier from the phone UI as a local administration process.

Related links

Setting the group identifier on page 149

Setting the group identifier

About this task

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

Procedure

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

   When you change the Group value, the phone restarts after you exit the admin menu.

6. Press **Save**.

Related links

Group identifier on page 149

Setting event logging

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 settings 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. Press **Save**.

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. Value operation: • 0: Disable enhanced local dialing for system numbers. • 1: Enable enhanced local dialing for system numbers.
ENHDIALSTAT	1	Specifies if the algorithm defined by the parameter is used during certain dialing behaviors. Value operation: • 0: Disables algorithm. • 1: Enables algorithm, but not for contacts. • 2: Enables algorithm, including contacts.
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. 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. This value must match the extension length set on your call server. Valid values are from 3 to 13.
PHNIC	011	Specifies the international access code. 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. 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. For example, 800-555-1111 has a length of 10. Valid values are from 5 to 15.
PHNOL	9	Specifies the outside line access code.

Table continues…

Parameter name	Default value	Description
		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.

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** > **Admin**.
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.

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 autogenerated `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** > **Admin**.
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 server**
6. Press **Select** or **OK** to change any of the following SIP global settings:
   - **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.

- **No**: Does not detect the Avaya environment and switches to a non-AST mode.

- **Reg. 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.

- **Proxy policy**: Specifies whether the settings of SIP proxy servers are read-only or can be edited by the user.

  The two modes are as follows:

  - **Auto**: The user can only view the settings.
  - **Manual**: The user can edit, delete, or create new server properties.

7. Select **SIP proxy server** 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. Press **Details** and use the **Up** and **Down Arrow** keys to view, add, or change the following settings:

   - **Proxy**: Specifies the IP address or DNS for Avaya Aura® Session Manager deployments. The corresponding parameter is SIP_CONTROLLER_LIST.
   - **Protocol**: Specifies the type of protocol. The options are TCP, UDP, or TLS. The corresponding parameter is SIPSIGNAL.
   - **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. If Transport Type is UDP/ TCP, the corresponding parameter is SIP_PORT_ SECURE.

9. Press **Save**.

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 administation 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.

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.

VIEW field description

Setting	Description	Associated Configuration Parameter
Model	The model of the phone that is set by factory procedures.	MODEL
Backup SW version	The version of the software backup.	
Gateway	The address of the gateway.	

Table continues…

Setting	Description	Associated Configuration Parameter
Group	The group identifier to download during start-up a specific configuration set for a dedicated user group.	GROUP
MAC	The MAC address of the phone.	MACADDR
Serial number	The serial number of the phone.	
SIP Proxy Server	The SIP proxy server to which the phone registered successfully.	SIPPROXYSRVR_IN_ USE
Presence Server The setting is only available in an Avaya Aura® environment.	The IP address of the presence server.	
HTTPS Server	The list of IP or DNS addresses of TLS servers for HTTPS file download, settings file or language files, during startup procedure.	TLSSRVR
HTTP Server	The IP address of the HTTP server that the phone accessed before successfully.	HTTPSRVR_IN_USE
DNS Server	The IP address of the DNS server that the phone accessed before successfully.	DNSSRVR_IN_USE
SW version	The version of the software.	
Protocol	Signaling protocol in effect, such as SIP.	

Setting the 802.1x operational mode

Before you begin

Set the following parameters:

- DOT1X: To support 802.1X Pass-thru operation, set the parameter to zero or one.
- DOT1XSTAT: To support supplicant operation, set the parameter to one or two.

Procedure

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

The phone displays the following settings:

- **Supplicant**
- **Pass-thru mode**

5. Select the setting that you want to change.
6. Press the **Change** softkey or the **Left** and **Right Arrow** keys to cycle through the following settings:
   - For the Pass-thru mode:
     - **On**: If DOT1X = 0
     - **On & proxy logoff**: If DOT1X = 1
     - **Off**: If DOT1X = 2
   - For the Supplicant:
     - **Disabled**: If DOT1XSTAT = 0
     - **Unicast**: If DOT1XSTAT = 1
     - **Multicast**: If DOT1XSTAT = 2
7. Press **Save**.

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

Chapter 9: Feature configuration

You can configure basic and advanced telephony features for phone users. The features can be configured locally, in the `Settings` file, or on the telephony feature server, such as Avaya Aura®. Users can access the list of currently active features on the Features screen.

Contacts list

With the enabled Contacts list feature, the end user can view, add and edit the list of numbers, and make calls by selecting a contact name or a number. The user can also create a local Contacts group with the numbers added to the Contacts list, add and remove contacts from the Groups list.

Configuring Groups list by using the web interface

Procedure

1. Log in to the web interface as an administrator.
2. In the navigation pane, click **Settings**.
3. In the **Group Number** field, specify the group numbers if available. The value must be between 0 and 99.

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.

Table continues…

Parameter name	Default value	Description
		Value Operation: • 0: No. The phone disables the **Contacts** option on the interface. • 1: Yes **Note:** The parameter is set to 1 in IP Office 10.1 or later. In previous releases it is set to 0.
ENABLE_MODIFY_CONTACTS		Specifies if the list of contacts and the function of the contacts application can be modified on the phone. Value Operation: • 0: No • 1: Yes
USER_STORE_URI		Specifies the URI path of HTTP/ HTPPS server for storing user data.

Recents

The Recent feature is used to access the call log on the phone. From the call log, you can do the following :

- View the call history details.
- Place a call.
- Delete a call record.
- Clear the Recent list.
- Add a contact.

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 up on which soft key on the Avaya J129 IP Phone screen. The options are: • 0 = Redial • 1 = Contacts • 2 = Emergency • 3 = Recents • 4 = Voicemail **Note:** Emergency calls are not supported in the 3PCC environment.

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. The options are: • 0: Disabled • 1: Enabled **Note:** This parameter is set to 0 in an IP Officeand in third-party call control environment.
ALLOW_DND_SAC_LINK_CHANGE	0	Specifies whether to enable DND and SAC link button on the menu. The options are: • 0: To disable DND and SAC link button. • 1: To enable DND and SAC link button. **Note:** Only Avaya J169/J179 IP Phone supports this feature.
DND_SAC_LINK	0	Specifies whether to enable DND and SAC link button on the menu. The value of this parameter is used if the ALLOW_DND_SAC_LINK_CHANGE is set to 0 The options are: • 0: To enable DND, and not SAC. • 1: To enable DND and SAC. **Note:** Only Avaya J169/J179 IP Phone supports this feature.
PRESENCE_ACL_CONFIRM	0	Specifies the handling of a Presence ACL update with pending watchers.

Table continues…

Parameter name	Default Value	Description
		The options are: • 0: Auto confirm. Automatically send a PUBLISH to allow presence monitoring. This is the default value. • 1: Ignore.— Take no action This parameter is not supported in an IP Office environment.

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.

Note:

Avaya J139 IP Phone does not support the Calendar feature.

Calendar configuration

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

Parameter name	Default Value	Description
EXCHANGE_SERVER_LIST	Null	Specifies a list of one or more Exchange server IP addresses. Addresses can be in dotted-decimal or DNS name format, separated by commas without any intervening spaces. The list can contain up to 255 characters. **Note:** Only Avaya J169/J179 IP Phone support this parameter.

Table continues…

Parameter name	Default Value	Description
EXCHANGE_SERVER_MODE	3	Specifies the protocol to be used to contact Exchange servers. Value operation: • 1: Use WebDAV • 2: Use Exchange Web Services (EWS) • 3: Try EWS first, if that fails, try WebDAV.
EXCHANGE_SERVER_SECURE_MODE	1	Specifies if HTTPS should be used to contact Exchange servers. Value operation: • 0: Use HTTP • 1: Use HTTPS
ENABLE_EXCHANGE_REMINDER	0	Specifies whether or not exchange reminders will be displayed. Value operation: • 0: Not displayed • 1: Displayed
EXCHANGE_SNOOZE_TIME	5	Specifies the number of minutes in which a reminder must be displayed again after it is temporarily dismissed. Valid values are 0 through 60.
EXCHANGE_AUTH_USERNAME_FORMAT	0	Specifies the necessary format of the username for http authentication. Value operation: • 0: Office 2003/Office2016 username format. Username=<ExchangeUserDomain\ExchangeUserAccount> or Username=<ExchangeUserAccount> if <ExchangeUserDomain> is empty. • 1: Office 365 format. Username=<ExchangeUserAccount@Exch

Table continues…

Parameter name	Default Value	Description
		angeUserDomain> or Username= <ExchangeUserAccount> if <ExchangeUserDomain> is empty.
EXCHANGE_EMAIL_DOMAIN	Null	Specifies the Exchange email domain. 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. Valid values are 0 through 3600.
EXCHANGE_REMINDER_TIME	5	Specifies the number of minutes before an appointment at which a reminder will be displayed. Valid values are 0 through 60.
EXCHANGE_REMINDER_TONE	1	Specifies whether or not a tone will be generated the first time an Exchange reminder is displayed. Value operation: • 0: Tone not generated. • 1: Tone generated.
EXCHANGE_USER_DOMAIN	Null	Specifies the domain for the URL used to obtain Exchange contacts and calendar data. The parameter is used as a part of the user authentication. The value can contain 0 to 255 characters.
PROVIDE_EXCHANGE_CALENDAR	1	Specifies if menu items for exchange calendar are displayed. Value operation: • 0: Not displayed • 1: Displayed (default)
PROVIDE_EXCHANGE_CONTACTS	1	Specifies if menu items for exchange contacts are displayed. Value operation: • 0: Not displayed

Table continues…

Parameter name	Default Value	Description
		• 1: Displayed (default)
USE_EXCHANGE_CALENDAR	0	Specifies whether the Calendar synchronizes with the Microsoft Exchange. Value operation: • 0: To disable synchronization. • 1: To enable synchronization.

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. Valid values are integers from 1 to 12.
GUESTLOGINSTAT	0	Specifies whether the Guest Login feature is available to users. Value Operation: • 0: The feature is not available. • 1: The feature is availble..
GUESTWARNING	5	Specifies the number of minutes, before time specified by GUESTDURATION, that a warning of the automatic logoff is initially presented to the Guest or Visiting User. Valid values are integers from 1 to 15.

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. Valid values are from 0 to 63.
DSCPAUD_FO	41	Specifies the DSCP value for flash Override precedence or priority level voice call. Valid values are from 0 to 63.
DSCPAUD_IM	45	Specifies the DSCP value for immediate precedence or priority level voice call. Valid values are from 0 to 63.
DSCPAUD_PR	47	Specifies the DSCP value for priority precedence or priority level voice call. Valid values are from 0 to 63.
ENABLE_PRECEDENCE_SOFT KEY	1	Specifies that whether the precedence soft key is enabled or

Table continues…

Parameter name	Default value	Description
		not on the idle line appearances on Phone Screen. Value Operation: • 0: Disabled. • 1: Enabled.
ENABLE_MLPP	0	Specifies that whether the Multiple Level Precedence and Preemption (MLPP) is enabled or not. Value Operation: • 0: Disabled. • 1: Enabled.
MLPP_MAX_PREC_LEVEL	1	Specifies the maximum allowed precedence level for the user. Value Operation: • 1: Routine • 2: Priority • 3: Immediate • 4: Flash • 5: Flash Override
MLPP_NET_DOMAIN	Null	Specifies the MLPP network domain. Value Operation: • Null: No domain configured • DSN: DSN network. • UC: UC network.

Call Forward

The Call Forward feature is used to divert incoming calls to another number. The call forward types are:

- 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 not answered within a stipulated time to another number.

Enhanced Call Forward

Enhanced Call Forward feature is used to set rules on call forwarding. The rules can be set by entering the internal and external phone numbers in the corresponding call forward types.

Configuring Call Forwarding on the phone web interface

About this task

Use this procedure to enable or disable the Call Forwarding feature through the web interface of the phone.

Procedure

1. Log in to the web interface.
2. In the navigation pane, go to **Settings**.
3. Select **Feature access**.
4. In the **Call Forward** field, click one of the following:
   - **Allow**: To enable the call forward option.
   - **Do not allow**: To disable the call forward option.

Call Forwarding 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
CALLFWDADDR	—	Sets the address to which the calls are forwarded. Users can change or replace this administered value if CALLFWDSTAT is not 0. **Note:** This parameter is supported when failed over from Aura SM to a non-Aura survivable server, excluding BSM.
CALLFWDDELAY	—	Sets the number of ring cycles before the call is forwarded to the forward or coverage address. The default delay is one ring cycle.

Table continues…

Parameter name	Default value	Description
CALLFWDSTAT	0	Sets the call forwarding mode of the phone by totaling? the following values: • 0: Disables call forwarding. • 1: Permits unconditional call forwarding. • 2: Permits call forward on busy. • 4: Permits call forward/no answer. Example: If you set a value of 6, the phone enables call forwarding on a busy tone and on no answer. **Note:** This parameter is supported when failed over from Aura SM to a non-Aura survivable server (excluding BSM).
COVERAGEADDR	—	Sets the address to which calls are forwarded for the call coverage feature. Users can change or replace this administered value if CALLFWDSTAT is not 0. **Note:** This parameter is not supported in a third-party call control environment.

Call Pickup

The Call Pickup feature is used to 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 and answer a call.

With the Extended Call Pickup feature, a member of a pick-up group can also answer another pickup group’s call on their extension number.

Call pickup 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
CALL_PICKUP_INDICATION	3	Specifies the following call pickup indication types: • Audio • Visual • None

Call Park

The Call Park feature is used to put an active call on hold at a parking extension and to retrieve the same parked call from another phone in the organization.

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

Auto Intercom group code

If the Auto Intercom grp code is activated by the system administrator, the end user can call a specific intercom group. Dial Intercom feature can allow one user to call another user in a group by using a predefined extension.

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

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

Whisper Page

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

This feature must be activated on the 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.

Send All Calls

The Send All Calls (SAC) feature is used to redirect incoming calls to a predefined coverage number. You must set a number so that all incoming calls rings once at the user’s extension and then redirects to your assigned number.

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

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.

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.

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 be a part of multiple hunt groups.

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

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 call is unattended by the receiver.

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 will be deleted when a callback is initiated by pressing the **Call** softkey from the entry's Details screen.

Priority Call

With enabled Priority Call feature, an outgoing internal call can be placed with a distinctive ring to indicate that it needs immediate attention. This feature allows the end user to call an extension that is set to **Do not disturb** status.

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

Priority Call configuration

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

Parameter name	Default value	Description
RINGPRIORITY	3	Specifies which distinctive ring rate is really for a priority call.
PHONE_NUMBER_PRIORITY	mobile,work,home	Specifies the default phone number priority.

Voicemail

The Voicemail feature is used to dial the configured voice mail number to receive a voice message.

Note:

You must specify the voicemail number in the corresponding field in Avaya Aura® System Manager before starting installation of the phone.

Configuring Voicemail by using the web interface

About this task

To configure the Voicemail list using the web interface, do the following steps:

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 voice mail in a non-Avaya environment.
4. Click one of the following:
   - **Save**
   - **Reset to Default**
   - **Help**

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 will show up on which softkey on the Avaya J100 Series IP Phones screens. The features are defined as follows: • 0 = Redial • 1 = Contacts • 2 = Emergency • 3 = Recents • 4 = Voicemail **Note:** Emergency calls are not supported in the 3PCC environment.

Note:

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.

Calling party number blocking

With the Calling Party Number (CPN) Block feature the end user can prevent his number from displaying. The system administrator must activate this feature and override the default system setting to display the extension on outgoing calls.

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

Calling party number unblocking

The Calling Party Number (CPN) Unblock feature allows the end user to display his extension during calls. If the Calling Party Number Block feature has been activated by the system administrator it should be changed back using CPN Unblock to enable displaying the extension.

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

Chapter 10: 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. TheAvaya 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 connection to the primary proxy is lost

A list of all proxies is provided to the phone during initial configuration. This list serves two purposes:

- Specifies the SIP proxies that are used by the phone.
- Prioritizes the list of proxies into primary, secondary, and survivable proxies.

Initially, DHCP, LLDP, or the `46xxsettings.txt` file provides this list of prioritized proxies. After the phone connects to Session Manager, it receives a new prioritized list of proxies specified by System Manager. This list takes precedence over other sources. The list provided by System Manager is derived from the following three fields:

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

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

Simultaneous registration

Phones can register simultaneously with more than one proxy. This makes the method of redundancy quick and deterministic. While configuring the phones for redundancy with Avaya Aura®, set the parameter SIPREGPROXYPOLICY to Simultaneous. In fact, when the phone registers for the first time, the parameter SIPREGPROXYPOLICY is forced to simultaneously register. Also, you can use the parameter SIMULTANEOUS_REGISTRATIONS to specify the number of proxies required to support simultaneous registration.

Note:

All Session Manager and Branch Session Manager instances support simultaneous registration while 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, then the value of SIMULTANEOUS_REGISTRATIONS is 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. 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

instance

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, then the phone displays the `Limited Phone Service` message. The message either disappears by itself or can be cancelled by the user. Also, 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 in the form of 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`.

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. Valid values are from 4 to 3600.	NA
DISCOVER_AVAYA_ENVIRONMENT	1	Specifies dynamic feature set discovery. Value operation are: • 0: Non-Avaya environment. Does not auto-discover Avaya SIP Telephony (AST) support . • 1: Avaya environment. Auto-discovers AST support. The SIP proxy server or controller might not support AST.	NA
FAILBACK_POLICY		Specifies the policy in effect for recovery from failover. Value operation: • Admin: The phone waits for administrative intervention before failing back to a higher priority controller. • Auto: The phone periodically checks the availability of the primary controller and fails back to the primary controller if available.	Failback Policy The value set in System Manager overwrites the value in the `46xxsettings.txt` file.
FAST_RESPONSE_TIMEOUT	4	Specifies the number of seconds the phone will wait before terminating an invite transaction if no response is received. Valid values are from 0 to 32. Value operation: • 0: Timer is disabled	Timer B 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.

Table continues…

Parameter name	Default value	Description	System Manager parameter name
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. Valid values are from 10 to 36000.	Reactive Monitoring
REGISTERWAIT	900	Specifies the number of seconds for next re-registration to the SIP proxy. Valid values are from 30 to 86400 seconds.	Registration Expiry Timer 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. Valid values are from 4 to 3600.	NA
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.	NA

Table continues…

Parameter name	Default value	Description	System Manager parameter name
		Value operation: • 0: Proxy server information received from PPM is not used. • 1: Proxy server information received from PPM is used.	
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	3	Specifies the number of simultaneous Session Manager and Branch Session Manager registrations that the phone must maintain. Valid values are from 1 to 3. The value of this parameter must not be less than the number of core Session Manager instances in SIP_CONTROLLER_LIST.	NA
SIPREGPROXYPOLICY	alternate	Specifies whether the telephone will attempt to maintain one or multiple simultaneous registrations. Value operation: • 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 . • Simultaneous: The phone simultaneously registers to more than one SIP proxy controller at the same time.	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. Value operation: • 0: PSTN access prefix digit is not removed. • 1: PSTN access prefix digit is removed from the collected digit string before formulating the INVITE for delivery to the controller. 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. 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. Value operation: • 0: PSTN access prefix is retained in the outgoing number • 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

Table continues…

Parameter name	Default value	Description
		numbers with more flexibility when used together with the LOCAL_DIAL_AREA_CODE parameter .
LOCAL_DIAL_AREA_CODE		Specifies whether a user must dial the area code for calls within the same area code regions. Value operation: • 0: Users do not need to dial an area code. • 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 not supported.

Chapter 11: Maintenance

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 both phone and web admin passwords are lost, press the key in 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 is applicable to the phones in 3PCC 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.

Device upgrade process

1. During boot-up, the phone receives the file server address from DHCP, LLDP, or the device interface.
2. The phone contacts the provisioning server to download the firmware upgrade file, `J100Supgrade.txt`.
3. In `J100Supgrade.txt`, the APPNAME parameter contains the firmware version.
4. The phone compares the 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.

Note:

J100 Aura phones can be used in Aura, IPO, and 3PCC environments. J100 3PCC phones cannot be used in Aura and IPO environments.

User profile backup on Personal Profile Manager (PPM)

Phone supports data backup by saving all non-volatile user parameters on PPM . When the user logs in to any registered device, PPM restores all user data on the device.

Note:

PPM is only available in an Avaya Aura® environment.

User profile parameters for backup

The following table lists the parameters that are backed up on Personal Profile Manager (PPM).

Parameter	Default value	Description
CLICKS	1	Specifies if the phone button can generate click sounds.
OUTSIDE_CALL_RING_TYPE	1	Specifies the default outside call ring type.
CALL_PICKUP_INDICATION	3	Specifies the following call pickup indication types: • Audio • Visual • None
AMPLIFIED_HANDSET	0	Specifies whether the handset amplification is enabled.
AMPLIFIED_HANDSET_NOMINAL_LEVEL_CALL_END	0	Specifies whether to set the volume level in amplified mode to nominal when all calls end.
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 to activate call logging.
DEFAULT_CONTACTS_STORE	1	Specifies the account where all user contacts are added by default.
ENABLE_PHONE_LOCK	0	Specifies whether the **Lock** softkey and the Lock feature button are displayed on the phone.
SHOW_CALL_APPEARANCE_NUMBERS	0	Specifies whether for a user the device displays call appearance numbers in the call containers.

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

- Endpoint Diagnostics
  - The ability to remotely control IP phones, to assist end users with IP Phone configuration and troubleshooting.
  - The ability to remotely generate single and bulk test calls between IP phones.
  - The ability to remotely execute limited packet captures on IP phones to troubleshoot and diagnose IP phone network traffic.
- Network Monitoring
  - The ability to monitor multiple network segments for performance in terms of packet loss, jitter, and delay.

- The ability to monitor hop-by-hop QoS markings for voice and video traffic.

Note:

The root trusted certificate used for the SLA Mon™ server certificate must be added to the trusted certificate list administered using TRUSTCERTS.

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

Chapter 12: Troubleshooting

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

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

Note:

The root trusted certificate used for the SLA Mon™ server certificate must be added to the trusted certificate list administered using TRUSTCERTS.

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

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 Environ screen.
6. Use the **Left** arrow key to configure the Avaya Environ 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.

Chapter 13: Appendix

List of configuration parameters

Parameter name	Default value	Description
100REL_SUPPORT	1	Specifies whether the 100rel option tag is included in the SIP INVITE header field. Value Operation: • 0: The tag is not included. • 1: The tag is included.
A		
ADMIN_HSEQUAL	1	Specifies handset audio equalization standards compliance. This parameter impacts the phone only if the handset equalization is not set by the user or by the HSEQUAL local procedure for that phone. Value Operation: • 1: Use handset equalization that is compliant with TIA 810/920. • 2: Use handset equalization that is compliant with FCC Part 68 HAC requirements.
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.

Table continues…

Parameter name	Default value	Description
		Valid values are from 5 min. to 1440 min.
ADMIN_PASSWORD	27238	Specifies an access code for accessing the Admin menu. 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. **Note:** • If this parameter length is set below 6 or above 31 alphanumeric characters, then the parameter is treated as not defined. • If this parameter is set in the `46xxsettings.txt` file, then it replaces PROCPSWD parameter. • If you set ADMIN_PASSWORD in the Avaya Aura® System Manager you require at least Avaya Aura® System Manager 7.1.0. • 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.

Table continues…

Parameter name	Default value	Description
		Value Operation: • 0: Disables AGC for the handset. • 1: Enables AGC for the handset.
AGCHEAD	1	Specifies the status of Automatic Gain Control (AGC) for the headset. Value Operation: • 0: Disables AGC for the headset. • 1: Enables AGC for the headset.
AGCSPKR	1	Specifies the status of Automatic Gain Control (AGC) for the speaker. Value Operation: • 0: Disables AGC for the speaker. • 1: Enables AGC for the speaker.
ALLOW_DND_SAC_LINK_CHANGE	0	Specifies whether to enable DND and SAC link button in the menu. Value Operation: • 0: To disable DND and SAC link button. • 1: To enable DND and SAC link button. **Note:** Only Avaya J169/J179 IP Phone supports this feature.
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. Valid values are 16 through 3600. This parameter is not supported in IP Office environment as there is no subscription to Avaya-cm-feature-status.
AUDASYS	3	Specifies the audible alerting setting for the phone.

Table continues…

Parameter name	Default value	Description
		Value Operation: • 0: Turns off audible alerting. User cannot adjust ringer volume. • 1: Turns on audible alerting. User can adjust ringer volume, but cannot turn off audible alerting. • 2: Turns off audible alerting. User can adjust ringer volume and can turn off audible alerting. • 3: Turns on audible alerting. User can adjust ringer volume and can turn off audible alerting. **Note:** Avaya J129 IP Phone does not support this parameter.
AUDIOENV	0	Specifies the audio environment index and enables you to customize the phone's audio performance. Valid values are 0 through299. This parameter affects settings for AGC dynamic range and handset noise reduction thresholds. Always consult Avaya before changing this parameter.
AUDIOPATH	1	Specifies the audio path for the phone. Value Operation: • 1: For speaker. • 2: For headset.
AUDIOSTHD		Specifies the level of sidetone in the headset. Value Operation: • 0: Normal level for most users • 1: One level softer than normal • 2: Two levels softer than normal • 3: Three levels softer than normal • 4: Off which means inaudible

Table continues…

Parameter name	Default value	Description
		• 5: One level louder than normal **Note:** Only Avaya J169/J179 IP Phone supports this feature.
AUDIOSTHS	0	Specifies the level of sidetone in the handset. Value Operation: • 0: Normal level for most users • 1: Three levels softer than normal • 2: Inaudible • 3: One level softer than normal • 4: Two levels softer than normal • 5: Four levels softer than normal • 6: Five levels softer than normal • 7: Six levels softer than normal • 8: One level louder than normal • 9: Two levels louder than normal
AUTH		Specifies whether the script files are downloaded from an authenticated server over an HTTPS link. Value Operation: • 0: Optional • 1: Mandatory
AUTHCTRLSTAT	0	Specifies if the enhanced debugging capabilities can be activated from the SSH server by the Avaya technicians only. Value Operation: • 0: Enhanced debugging capabilities are disabled. • 1: Enhanced debugging capabilities are enabled. The parameter must be set to 1 only for the debugging period by Avaya technicians. Set the

Table continues…

Parameter name	Default value	Description
		parameter back to 0 when the debugging period completes.
BACKGROUND_IMAGE		Specifies custom background images that can be loaded from the provisioning server. Phone supports up to 5 background images with the following limitation: • Only jpeg format files are supported. • The maximum file size is 256 KB. • The file names are case sensitive. Example: SET BACKGROUND_IMAGE [xxx.jpg] **Note:** Avaya J139 IP Phone does not support Background image feature.
BACKGROUND_IMAGE_DISPLAY		Specifies the background image to be displayed. Note that, If BACKGROUND_IMAGE_SELECTABLE is set to 1 then the end user may override this setting.
BACKGROUND_IMAGE_SELECTABLE	1	Allows the end user to select background images. Value operations: • 0: The user can not use a background images from the phone UI. • 1: The user can select a background images from the phone UI.
BACKLIGHT_SELECTABLE	0	Specifies whether backlight timer is selected by the administrator (BAKLIGHTOFF) or user. Value operations: • 0: To set Backlight Timer value from `46xxsettings.txt` file.

Table continues…

Parameter name	Default value	Description
		• 1: To set Backlight Timer value according to user settings. **Note:** 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. Phones with gray-scale displays do not completely turn backlight off, they set it to the lowest non-off level. Valid values are 0 through 999. A value of 0 means that the display backlight will not be turned off automatically when the phone is idle. For ENERGY STAR compliance on applicable phones, a value of 20 is recommended.
BRANDING_VOLUME	5	Specifies the volume level at which the Avaya audio brand is played. Value Operation • 8: 9db above nominal • 7: 6db above nominal • 6: 3db above nominal • 5: nominal • 4: 3db below nominal • 3: 6db below nominal • 2: 9db below nominal • 1:12db below nominal
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**.
C		

Table continues…

Parameter name	Default value	Description
CALL_TRANSFER_MODE	0	Determines the call transfer mode in 3rd party environments. Valid value is 0 or 1.
CALLFWDADDR The parameter is only available in an Avaya Aura® environment.	Null	Sets the address to which calls are forwarded for the call forwarding feature. Users can change or replace this administered value if CALLFWDSTAT is not 0.
CALLFWDDELAY The parameter is only available in an Avaya Aura® environment.		Sets the number of ring cycles before the call is forwarded to the forward or coverage address. The default delay is one ring cycle.
CALLFWDSTAT The parameter is only available in an Avaya Aura® environment.	0	Sets the call forwarding mode of the phone by summing the following values: • 1: Permits unconditional call forwarding. • 2: Permits call forward on busy. • 4: Permits call forward/no answer. • 0: Disables call forwarding. Example: a value of 6 allows call forwarding on busy and on no answer.
CERT_WARNING_DAYS	60	Specifies the number of days before the expiration of a certificate that a warning will first appear on the phone screen. Certificates include trusted certificates, OCSP certificates and identity certificate. Log and syslog message will also be generated. The warning will reappear every seven days.Valid values are from 0 to 99. Value operation: • 0: No certificate expiration warning will be generated.
CERT_WARNING_DAYS_EASG	365	Specifies how many days before the expiration of EASG product certificate that a warning should first appear on the phone screen.

Table continues…

Parameter name	Default value	Description
		Syslog message will be also generated. Valid values are from 90 to 730.
CNGLABEL	1	Determines if personalize button labels can be displayed to the user. Value Operation: • 0: Capability not displayed to the user. • 1: Capability displayed to the user.
CONF_TRANS_ON_PRIMARY_APPR	0	Determines conference and transfer setup whether to use idle primary call appearance or idle bridged call appearance. Value Operation: • 0: To specify conference and transfer setup to use an idle primary call appearance at first attempt. However, if an idle primary call appearance is unavailable, then the setup will use idle bridged call appearance regardless of the setting of AUTO_SELECT_ANY_IDLE_APPR. If a bridged call appearance initiates the setup, then setup will use idle bridged call appearance of same extension. If an idle bridged call appearance of the same extension is not available and AUTO_SELECT_ANY_IDLE_APPR is set to 1, then setup will use any idle call appearance. However, if AUTO_SELECT_ANY_IDLE_APPR is set to 0 and if same bidged call extension is not available, the setup initiated on a bridged call appearance will be denied. • 1: To specify conference and transfer setup to use an idle primary call appearance at first attempt. However, if an idle

Table continues…

Parameter name	Default value	Description
		primary call appearance is unavailable, then the setup will use idle bridged call appearance. If a bridged call appearance initiates the setup, then setup will use idle bridged call appearance of either the same extension or different extension. AUTO_SELECT_ANY_IDLE_APPR is ignored. **Note:** Only Avaya J169/J179 IP Phone supports this feature.
CONFERENCE_FACTORY_URI	Null	Specifies the URI for Avaya Aura Conferencing. Valid values contain zero or one URI, where a URI consists of a dial string followed by @, and then the domain name, which must match the routing pattern configured in System Manager for Adhoc Conferencing. Depending on the dial plan, the dial string can need a prefix code, such as a 9 to get an outside line. The domain portion of the URI can be in the form of an IP address or an FQDN. The value can contain 0 to 255 characters. The default value is null.
CONFERENCE_TYPE	1	Determines the selection of the Conference Method. Value Operation: • 0: Local conferencing is supported based on sipping services. • 1: Server based conferencing is supported. • 2: Click-to conference server based conferencing is supported.

Table continues…

Parameter name	Default value	Description
		If the parameter is set to a value that is outside the range then default value is selected. **Note:** The parameter is set to 0 in IP Office environment.
CONFIG_SERVER	Null	Specifies the address of the Avaya configuration server. Valid values contain zero or one IP address in dotted decimal or DNS name format, optionally followed by a colon and a TCP port number. The value can contain 0 to 255 characters. The default value is null. This parameter is not supported in IP Office environment as PPM is not supported.
CONFIG_SERVER_SECURE_MODE	1	Specifies whether HTTP or HTTPS is used to access the configuration server. Value Operation: • 0: HTTP • 1: HTTPS • 2: Use HTTPS if SIP transport mode is TLS, otherwise use HTTP. This parameter is not supported in IP Office environment as PPM is not supported.
CONTACT_NAME_FORMAT	0	Specifies how contact names are displayed. Value operation • 0: The name format is Last name, First name. • 1: The name format is First name, Last name.
CONTROLLER_SEARCH_INTERVAL	16	Specifies the number of seconds the phone will wait to complete the

Table continues…

Parameter name	Default value	Description
		maintenance check for monitored controllers. Valid values are 4 through 3600.
COUNTRY		Used for network call progress tones. • For Argentina use keyword Argentina. • For Australia use keyword Australia. • For Brazil use keyword Brazil. • For Canada use keyword USA. • For France use keyword France. • For Germany use keyword Germany. • For Italy use keyword Italy. • For Ireland use keyword Ireland. • For Mexico use keyword Mexico. • For Spain use keyword Spain. • For United Kingdom use keyword UK. • For United States use keyword USA. Country names with spaces must be enclosed in double quotes.
COVERAGEADDR	Null	Sets the address to which calls will be forwarded for the call coverage feature. Users can change or replace this administered value if CALLFWDSTAT is not 0.
D		
DATEFORMAT		Specifies the format for dates displayed in the phone. • Use %d for day of month • Use %m for month in decimal format.

Table continues…

Parameter name	Default value	Description
		• Use %y for year without century (For example, 07). • Use %Y for year with century (For example, 2007). Any character not preceded by % is reproduced exactly.
DAYLIGHT_SAVING_SETTING_MODE		Specifies daylight savings time setting for phone. Value Operation: • 0: Daylight saving time not activated • 1: Daylight saving time is activated. Time set to DSTOFFSET. • 2: Activates automatic daylight savings adjustment as specified by DSTSTART and DSTSTOP.
DELETE_MY_CERT	0	Specifies whether the installed identity certificate, using SCEP or PKCS12 file download, will be deleted. • 0: Installed identity certificate remains valid. • 1: Installed identity certificate is removed.
DES_STAT	2	Specifies if DES discovery is to be attempted during the boot process if there is no configuration file server provisioned on the phone. Value operation: • 0: DES discovery is disabled and can only be restored with Reset to Defaults • 1: DES discovery is disabled • 2: DES discovery is enabled
DHCPSTD	0	Specifies whether DHCP complies with the IETF RFC 2131 standard.

Table continues…

Parameter name	Default value	Description
		Value Operation: • 0: Continue using the address in an extended rebinding state. • 1: Immediately stop using the address.
DIALPLAN	Null	Specifies the dial plan used in the phone. Dialplan accelerates dialing by eliminating the need to wait for the INTER_DIGIT_TIMEOUT timer to expire. The value can contain 0 to 1023 characters. The default value is null.
DISCOVER_AVAYA_ENVIRONMENT		Specifies dynamic feature set discovery Value Operation: • 1: The phone discovers and verifies if the controller supports the AST feature set or not. The phone sends a SUBSCRIBE request to the active controller for the Feature Status Event Package (avaya-cm-feature-status). If the request succeeds, the phone proceeds with PPM Synchronization. If the request is rejected, or is proxied back to the phone, or does not receive a response, the phone assumes that AST features are not available. • 0: The phone operates in a mode where AST features are not available. **Note:** Set the parameter to 0 for IP Office environment.
DISPLAY_SSL_VERSION	0	Specifies whether OpenSSL and OpenSSH versions are displayed in the **Administration** menu.

Table continues…

Parameter name	Default value	Description
		Value Operation: • 0: OpenSSL and OpenSSH versions are not displayed. • 1: OpenSSL and OpenSSH versions are displayed.
DND_SAC_LINK	0	Specifies whether to enable DND and SAC link button in the menu. The value of this parameter is used if the ALLOW_DND_SAC_LINK_CHANGE is set to 0 Value Operation: • 0: To enable DND, and not SAC. • 1: To enable DND and SAC. **Note:** Only Avaya J169/J179 IP Phone supports this feature.
DNSSRVR		Domain Name Server for Access Profile 2
DOMAIN	Null	Specifies a character string that will be appended to parameter values that are specified as DNS names, before the name is resolved. The value can contain 0 to 255 characters. The default value is null.
DOT1X		Specifies the 802.1X pass-through operating mode. Pass-through is the forwarding of EAPOL frames between the phone's ethernet line interface and its secondary (PC) ethernet interface Value Operation: • 0: EAPOL multicast pass-through enabled without proxy logoff. • 1: EAPOL multicast pass-through enabled with proxy logoff.

Table continues…

Parameter name	Default value	Description
		• 2: EAPOL multicast pass-through disabled.
DOT1XEAPS	MD5	Specifies the authentication method to be used by 802.1X. Valid values are MD5, and TLS.
DOT1XSTAT	0	Specifies the 802.1X supplicant operating mode. Value Operation: • 0: Supplicant disabled. • 1: Supplicant enabled, but responds only to received unicast EAPOL messages. • 2: Supplicant enabled; responds to received unicast and multicast EAPOL messages.
DSCPAUD	46	Specifies the layer 3 Differentiated Services (DiffServ) Code Point for audio frames generated by the phone. Valid values are from 0 to 63. This parameter can also be set through the LLDP, which overwrites any value set in this file.
DSCPAUD_FL	43	Specifies the DSCP value for flash precedence or priority level voice call. Valid values are from 0 to 63.
DSCPAUD_FO	41	Specifies the DSCP value for flash Override precedence or priority level voice call. Valid values are from 0 to 63.
DSCPAUD_IM	45	Specifies the DSCP value for immediate precedence or priority level voice call. Valid values are from 0 to 63.
DSCPAUD_PR	47	Specifies the DSCP value for priority precedence or priority level voice call. Valid values are from 0 to 63.

Table continues…

Parameter name	Default value	Description
DSCPMGMT	16	Specifies the DSCP value for OA&M management packet. Valid values are from 0 to 63.
DSCPSIG	34	Specifies the layer 3 Differentiated Services (DiffServ) Code Point for signaling frames generated by the phone. Valid values are 0 through 63. This parameter can also be set through LLDP, which overwrites any value set in this file.
DSCPVID	34	Specifies the layer 3 Differentiated Services (DiffServ) Code Point for video frames generated by the phone. Valid values are 0 through 63. The default value is 34.
DSTOFFSET	1	Specifies the time offset in hours of daylight savings time from local standard time. Valid values are 0, 1, or 2. The default value is 1.
DSTSTART	2SunMar2L	Specifies when to apply the offset for daylight savings time. The default value is 2SunMar2L (the second Sunday in March at 2AM local time).
DSTSTOP	1SunNov2L	Specifies when to stop applying the offset for daylight savings time. The default value is 1SunNov2L (the first Sunday in November at 2AM local time).
DTMF_PAYLOAD_TYPE	120	Specifies the RTP payload type to be used for RFC 2833 signaling. Valid values are 96 through 127.
E		
EASG_SITE_AUTH_FACTOR	Null	Specifies Site Authentication Factor code associated with the EASG site certificate being installed. Valid

Table continues…

Parameter name	Default value	Description
		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. This parameter is supported by only Avaya J129 IP Phone. Value operation: • 0: EEE is disabled on both PHY1 and PHY2. • 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. Value operation: • 0: Disable ELD for System Numbers • 1: Enable ELD for System Numbers **Note:** Avaya J139 IP Phone does not support Busy Indicator feature.
ENABLE_3PCC_ENVIRONMENT	1	Specifies that the phone is working in the Third-party call control setup environment. Value Operation • 0: Disabled • 1: Enabled

Table continues…

Parameter name	Default value	Description
		Set the parameter to 0 for Avaya Aura® and IP Office environment.
ENABLE_AUTO_ANSWER_SUPPORT	0	Specifies that the auto-answer feature is enabled. Value Operation • 0: Disabled • 1: Enabled **Note:** This parameter is only applicable if a 3PCC environment is configured.
ENABLE_AVAYA_ENVIRONMENT	1	Specifies whether the phone is configured to be used in an Avaya (SES) or a third-party proxy environment. Value Operation: • 0: Configured for 3rd party proxy with SIPPING 19 features. • 1: Configured for Avaya environment with AST features and PPM. **Note:** Set the parameter to 0 for IP Office environment.
ENABLE_BLIND_TRANSFER	1	Specifies that whether the blind transfer is enabled or not. Value Operation: • 0: Disabled. • 1: Enabled.
ENABLE_CALL_LOG		Species if call logging and associated menus are available on the phone. Value Operation: • 0: No • 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. Value Operation: • 0: No. The phone disables the **Contacts** option on the interface. • 1: Yes **Note:** The parameter is set to 1 in IP Office 10.1 or later. In previous releases it is set to 0.
ENABLE_DND	1	Specifies that the do-not-disturb feature is enabled. Value Operation • 0: Disabled • 1: Enabled **Note:** This parameter is only applicable if a 3PCC environment is configured.
ENABLE_DND_PRIORITY_OVER_CFU_CFB	0	Specifies that the Do-not-disturb (DND) feature is given priority over Call forwarding unconditionally (CFU) and Call forwarding busy (CFB). Value Operation • 0: Disabled • 1: Enabled **Note:** This parameter is only applicable if a 3PCC environment is configured.
ENABLE_EARLY_MEDIA		Specifies if the phone sets up a voice channel to the called party before the call is answered. Value Operation: • 0: No

Table continues…

Parameter name	Default value	Description
		• 1: Yes Setting this parameter to 1 can speed up call setup.
ENABLE_EXCHANGE_REMINDER	0	Specifies whether or not exchange reminders will be displayed. Value Operation: • 0: Not displayed • 1: Displayed
ENABLE_G711A	1	Specifies if the G.711 a-law codec is enabled. Value Operation: • 0: Disabled • 1: Enabled
ENABLE_G711U	1	Specifies if the G.711 mu-law codec is enabled. Value Operation: • 0: Disabled • 1: Enabled
ENABLE_G722	1	Specifies if the G.722 codec is enabled. Value Operation: • 0: Disabled • 1: Enabled
ENABLE_G726	1	Specifies if the G.726 codec is enabled. Value Operation: • 0: Disabled • 1: Enabled
ENABLE_G729	1	Specifies if the G.729A codec is enabled. Value Operation: • 0: Disabled • 1: Enabled without Annex B support (default). • 2: Enabled with Annex B support.

Table continues…

Parameter name	Default value	Description
ENABLE_IPOFFICE	0	Specifies whether the J100 phone can operate in 2 different modes with IP Office. The first mode allows native support of the J100 phone with IP Office with a limited feature set. The second mode allows support of the J100 phone with additional feature support driven by the IP Office proxy. Value Operation: • 0: The phone does not support IP Office (except in Avaya Aura failover mode). • 1: The phone supports IP Office in a native environment. • 2: The phone supports IP Office with additional features driven by the IP Office proxy Avaya J129 IP Phone supports value 0 and 1. Avaya J139 IP Phoneand Avaya J169/J179 IP Phonesupports value 0 and 2.
ENABLE_MLPP	0	Specifies that whether the Multiple Level Precedence and Preemption (MLPP) is enabled or not. Value Operation: • 0: Disabled. • 1: Enabled.
ENABLE_MODIFY_CONTACTS		Specifies if the list of contacts and the function of the contacts application can be modified on the phone. Value Operation: • 0: No • 1: Yes
ENABLE_MULTIPLE_CONTACT_WARNING		Specifies if a warning message must be displayed if there are multiple phones registered on a user's behalf.

Table continues…

Parameter name	Default value	Description
		Value Operation: • 0: No • 1: Yes **Note:** Multiple registered phones can lead to service disruption.
ENABLE_OOD_MSG_TLS_ONLY	1	Specifies if an Out-Of-Dialog (OOD) REFER must be received over TLS transport to be accepted. Value Operation: • 0: No, TLS is not required. • 1: Yes, TLS is required. **Note:** A value of 0 is only intended for testing purposes.
ENABLE_OPUS	1	Specifies if the OPUS codec capability of the phone is enabled or disabled. Value Operation: • 0: Disabled. • 1: Enabled OPUS wideband with bitrate of 20KBps. • 2: Enabled OPUS narrowband with bitrate of 16KBps. • 3: Eanbled OPUS narrowband with bitrate of 12KBps. **Note:** Avaya J129 IP Phone does not support third-party local call conference with OPUS.
ENABLE_PHONE_LOCK	0	Specifies whether the **Lock** softkey on the Idle phone screen and the **Lock** feature button are enabled on the phone. If enabled, a user can manually lock the phone by pressing the button or selecting the feature.

Table continues…

Parameter name	Default value	Description
		Value operation: • 0: Disabled. **Lock** softkey and feature button are not displayed. • 1: Enabled. **Lock** softkey and feature button are displayed. **Note:** On Avaya J129 IP Phone, the **Lock** option is in the **Main menu**. There is no **Lock** softkey or feature button.
ENABLE_PPM_SOURCED_SIPPROXYSRVR The parameter is only available in an Avaya Aura® environment.	1	Enables PPM as a source of SIP proxy server information. Value Operation: • 0: Proxy server information received from PPM is not used. • 1: Proxy server information received from PPM is not used.
ENABLE_PRECEDENCE_SOFTKEY	1	Specifies that whether the precedence soft key is enabled or not on the idle line appearances on Phone Screen. Value Operation: • 0: Disabled. • 1: Enabled.
ENABLE_PRESENCE	1	Specifies if presence will be supported. Value Operation: • 0: Disabled • 1: Enabled **Note:** 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

Table continues…

Parameter name	Default value	Description
		Value operation: • 0: Embedded public CA certificates are only trusted when TRUSTCERTS is empty. • 1: Embedded public CA certificates are always trusted.
ENABLE_RECORDING	0	Specifies if audio debug recording is enabled for users. Value Operation: • 0: Audio debug recording is disabled. • 1: Audio debug recording is enabled.
ENABLE_REDIAL		Specifies if **Redial** softkey is available. Value Operation: • 0: No • 1: Yes
ENABLE_REDIAL_LIST		Specifies if the phone redials last number or displays list of recently dialed numbers. Value Operation: • 0: Last number redial • 1: User can select between the last redialled number and the redial list. • **Note:** Avaya J139 IP Phone does not support this feature.
ENABLE_REMOVE_PSTN_ACCESS_PREFIX		Allows phone to perform digit manipulation during failure scenarios. This parameter allows removal of PSTN access prefix from the outgoing number.

Table continues…

Parameter name	Default value	Description
		Value Operation; • 0: PSTN access prefix is retained in the outgoing number. • 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. Value Operation: • 0: **Emergency** softkey is not displayed. • 1: **Emergency** softkey is displayed without a confirmation screen. • 2: **Emergency** softkey is displayed with a confirmation screen. **Note:** 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. All emergency numbers will always be supported. Value Operation: • 0: **Emergency** softkey is not displayed. • 1: **Emergency** softkey is displayed without a confirmation screen. • 2: **Emergency** softkey is displayed with a confirmation screen.

Table continues…

Parameter name	Default value	Description
		Note: The parameter is set to 0 for IP Office environment.
ENABLE_SIP_USER_ID	0	Specifies that the **SIP User ID** field is required under **ADMIN** > **SIP** > **SIP Global Settings**. Value Operation • 0: Disabled • 1: Enabled
ENABLE_STRICT_USER_VALIDATION	0	Specifies that the validation is done for the **To header** and **Request-URI** against AOR and **Contact** header during phone registration. Value Operation • 0: No validation. • 1: Validates the phone registration.
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. Value Operation: • 0: SRTCP is disabled. • 1: SRTCP is enabled.
ENFORCE_SIPS_URI	1	Specifies if a SIPS URI must be used for SRTP. Value Operation: • 0: Not enforced • 1: Enforced
ENHDIALSTAT	1	Specifies if the algorithm defined by the parameter is used during certain dialing behaviors.

Table continues…

Parameter name	Default value	Description
		Value Operation: • 0: Disables algorithm. • 1: Enables algorithm, but not for contacts. • 2: Enables algorithm including contacts. **Note:** 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. Value Operation: • 0: Calling Party Name is used. • 1: VDN or the skill name is used.
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. Valid values are 0 through 1000. This parameter is used only for development and debugging purposes.
EXCHANGE_AUTH_USERNAME_FORMAT	0	Specifies the necessary format of the username for http authentication. Value operation: • 0: Office 2003/Office2016 username format. Username=<ExchangeUserDomain\ExchangeUserAccount> or Username=<ExchangeUserAccount> if <ExchangeUserDomain> is empty. • 1: Office 365 format. Username=<ExchangeUserAccount@ExchangeUserDomain> or Username=<ExchangeUserAccount> if

Table continues…

Parameter name	Default value	Description
		<ExchangeUserDomain> is empty.
EXCHANGE_EMAIL_DOMAIN	Null	Specifies the Exchange email domain. 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. Valid values are 0 through 3600.
EXCHANGE_REMINDER_TIME	5	Specifies the number of minutes before an appointment at which a reminder will be displayed. Valid values are 0 through 60.
EXCHANGE_REMINDER_TONE	1	Specifies whether or not a tone will be generated the first time an Exchange reminder is displayed. Value Operation: • 0: Tone not generated. • 1: Tone generated.
EXCHANGE_SERVER_LIST	Null	Specifies a list of one or more Exchange server IP addresses. Addresses can be in dotted-decimal or DNS name format, separated by commas without any intervening spaces. The list can contain up to 255 characters.
EXCHANGE_SERVER_SECURE_MODE	1	Specifies if HTTPS should be used to contact Exchange servers. Value Operation • 0: Use HTTP • 1: Use HTTPS
EXCHANGE_SNOOZE_TIME	5	Specifies the number of minutes in which a reminder must be displayed again after it is temporarily dismissed. Valid values are 0 through 60.

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. The value can contain 0 to 255 characters.
EXTEND_RINGTONE	Null	Provides a way to customize ring tone files. This is a comma separated list of file names in xml format.
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. Valid values are 5 through 999.
FAST_RESPONSE_TIMEOUT	4	Specifies the number of seconds the phone will waits before terminating an INVITE transaction if no response is received. Valid values are 0 through 32. Value of 0 means that this timer is disabled.
FIPS_ENABLED	0	Specifies whether only FIPS-approved cryptographic algorithms will be supported. Value Operation: • 0: No restriction on using non FIPS-approved cryptographic algorithms. • 1: Use only FIPS-approved cryptographic algorithms using embedded FIPS 140-2-validated cryptographic module.
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

Table continues…

Parameter name	Default value	Description
		available on the called or remote party. Valid values are from 5 to 20 seconds.
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. Valid values are 8 to 31 alphanumeric characters.
FQDN_IP_MAP	Null	Specifies a comma separated list of name or value pairs where the name is an FQDN and the value is an IP address. The IP address may be IPv6 or IPv4 but the value can only contain one IP address. String length is up to 255 characters without any intervening spaces inside the string. The purpose of this parameter is to support cases where the server certificate Subject Common Name of Subject Alternative Names includes FQDN, instead of IP address, and the SIP_CONTROLLER_LIST is defined using IP address. This parameter is supported with phone service running over TLS, however, the main use case is for Avaya Aura SM/PPM services. This parameter must not to be used as an alternative to a DNS lookup or reverse DNS lookup.
G		
G726_PAYLOAD_TYPE	110	Specifies the RTP payload type to be used for the G.726 codec. Valid values are 96 through 127.

Table continues…

Parameter name	Default value	Description
GMTOFFSET	0:00	Specifies the time offset from GMT in hours and minutes. The format begins with an optional + or - (+ is assumed if omitted), followed by 0 through 12 (hours), followed by a colon (:), followed by 00 through 59 (minutes).
GROUP	0	Specifies specifically-designated groups of phones by using IF statements based on the GROUP parameter. The value of GROUP can be set manually in a phone by using the GROUP local admin procedure. 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. Valid values are integers from 1 to 12.
GUESTLOGINSTAT	0	Specifies whether the Guest Login feature is available to users. Value Operation: • 0: The feature is not available. • 1: The feature is availble..
GUESTWARNING	5	Specifies the number of minutes, before time specified by GUESTDURATION, that a warning of the automatic logoff is initially presented to the Guest or Visiting User. Valid values are integers from 1 to 15.
H		
HANDSET_PROFILE_DEFAULT	1	Specifies the number of the default handset audio profile. Valid values are 1 through 20.

Table continues…

Parameter name	Default value	Description
HANDSET_PROFILE_NAMES	Null	Specifies an ordered list of names to be displayed for handset audio profile selection. The list can contain 0 to 255 UTF-8 characters. Names are separated by commas without any intervening spaces. Two commas in succession indicate a null name, which means that the default name should be displayed for the corresponding profile. Names might contain spaces, but if any do, the entire list must be quoted. There is no way to prevent a profile from being displayed.
HEADSET_PROFILE_DEFAULT	1	Specifies the number of the default headset audio profile. Valid values are 1 through 20.
HEADSET_PROFILE_NAMES	Null	Specifies an ordered list of names to be displayed for headset audio profile selection. The list can contain 0 to 255 UTF-8 characters. Names are separated by commas without any intervening spaces. Two commas in succession indicate a null name, which means that the default name is displayed for the corresponding profile. Names can contain spaces, but if any do, the entire list must be quoted. There is no way to prevent a profile from being displayed.
HEADSYS	0	Specifies whether the phone goes on-hook if the headset is active when the disconnect message is received. Value Operation: • 0: The phone goes on-hook if the disconnect message is received when the headset is active. • 1: Disconnect messages are ignored when the headset is

Table continues…

Parameter name	Default value	Description
		active. This is used for Call Center setting.
HOMEIDLETIME	10	Specifies the number of minutes of idle time after which the **Home** screen is displayed. Valid values are 0 through 30. A value of 0 means that the **Home** screen is not displayed automatically when the phone is idle. **Note:** Only Avaya J129 IP Phone supports this feature.
HTTPEXCEPTIONDOMAINS	Null	Specifies a list of one or more domains, separated by commas without any intervening spaces, for which HTTPPROXY is not used. The value can contain 0 to 255 characters. The default value is null.
HTTPPORT	80	Sets the TCP port used for HTTP file downloads from non-Avaya servers. 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. Valid value can contain zero or one IP address in dotted decimal or DNS name format, optionally followed by a colon and a TCP port number. The value can contain 0 to 255 characters.
HTTPSRVR	Null	Specifies zero or more HTTP server IP addresses to download configuration script files. The addresses must be separated by commas without any intervening

Table continues…

Parameter name	Default value	Description
		spaces. The format of specifying IP addresses are: • Dotted decimal • Colon-hex • DNS name The parameter can be set by using LLDP. Valid values contains 0 to 255 ASCII characters.
I		
ICMPDU		Specifies if ICMP Destination Unreachable messages are generated. Value Operation: • 0: No messages are generated. • 1: Limited port unreachable messages are generated. • 2: Protocol and port unreachable messages are generated.
ICMPRED		Specifies if received ICMP Redirect messages are processed. Value Operation: • 0: No • 1: Yes
INGRESS_DTMF_VOL_LEVEL	-12dBm	Specifies the power level of tone, expressed in dBm0. Values can range from -20dBm to -7dBm.
INSTANT_MSG_ENABLED	1	Specifies whether Instant Messaging is enabled or disabled. Value Operation: • 0: Disabled • 1: Enabled
INTER_DIGIT_TIMEOUT	5	Specifies the number of seconds that the phone waits after a digit is dialed before sending a SIP INVITE.

Table continues…

Parameter name	Default value	Description
		Valid values are 1 through 10.
IPV6DADXMITS	1	Specifies whether Duplicate Address Detection is performed on tentative addresses, as specified in RFC 4862. Value operation: • 0: DAD is disabled • 1 to 5: Maximum number of transmitted Neighbor Solicitation messages.
IPV6STAT	0	Specifies whether IPv6 will be supported or not. Value operation: • 0: IPv6 will not be supported. • 1: IPv6 will be supported.
K		
L		
L2Q	0	Specifies whether the VLAN tagging is enabled or disabled. Value Operation: • 0: Auto. VLAN tagging is turned on when the network can support VLAN tagging and L2QVLAN is non zero. • 1: On. VLAN tagging is turned on when the network can support VLAN tagging. The IP phone sends tagged frames with VLAN = L2QVLAN, even if L2QVLAN is set to 0. • 2: Off. VLAN functionality is disabled. **Note:** This parameter can also be set through: • Local admin procedure • A name equal to value pair in DHCPACK message

Table continues…

Parameter name	Default value	Description
		• SET command in a settings file • DHCP option 43 • LLDP
L2QAUD	6	Specifies the value of the VLAN priority portion of the VLAN tag when the phone generates tagged Ethernet frames from the internal CPU of the phone. These values are inserted into the VLAN tag for audio frames (RTP, RTCP, SRTP, SRTCP). All other frames except those specified by the L2QSIG parameter are set to priority 0. Valid values are 0 through 7. **Note:** This parameter can also be set through: • SET command in a settings file • LLDP
L2QSIG	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 signaling frames (SIP). All other frames except those specified by the L2QAUD parameter are set to priority 0. Valid values are 0 through 7. **Note:** This parameter can also be set through: • SET command in a settings file • LLDP

Table continues…

Parameter name	Default value	Description
L2QVLAN	0	Specifies the voice VLAN ID to be used by IP phones. Valid values are 0 through 4094. **Note:** This parameter can also be set through: • Local admin procedure • A name equal to value pair in DHCPACK message • SET command in a settings file • DHCP option 43 • LLDP
LANGUAGES		Specifies the language files that must be installed or downloaded to the phone. Filenames can be full URL, relative pathname, or filename. Valid values can contain 0 to 1096 ASCII characters, including commas. Filenames must end in `.xml`
LLDP_ENABLED	2	Specifies whether LLDP is enabled. Value operation: • 0: Disabled • 1: Enabled • 2: Enabled, but only begins transmitting if an LLDP frame is received.
LOCAL_DIAL_AREA_CODE		Specifies if user must dial area code for calls within same area code regions. Value Operations: • 0: User does not need to dial area code. • 1: User need to dial area code. When enabled, the area code

Table continues…

Parameter name	Default value	Description
		parameter (PHNLAC) should also be configured. **Note:** This parameter is supported when the phone is failed over.
LOCAL_LOG_LEVEL	3	Specifies the severity levels of events logged in the `endptRecentLog`, `endptResetLog`, and `endptStartupLog` objects in the SNMP MIB. Events with the selected severity level and above are logged. Lower numeric severity values correspond to higher severity levels Value Operation: • 0: Emergency events are logged. • 1: Alert and Emergency events are logged. • 2: Critical, Alert and Emergency events are logged. • 3: Error, Critical, Alert and Emergency events are logged (default). • 4: Warning, Error, Critical, Alert and Emergency events are logged. • 5: Notice, Warning, Error, Critical, Alert and Emergency events are logged. • 6: Informational, Notice, Warning, Error, Critical, Alert and Emergency events are logged. • 7: Debug, Informational, Notice, Warning, Error, Critical, Alert and Emergency events are logged **Warning:** Setting the value to 7 can impact the performance of the

Table continues…

Parameter name	Default value	Description
		phone because of the number of events generated.
LOCALLY_ENFORCE_PRIVACY_HEADER 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. Value Operation: • 0: Disabled. CallerID information is displayed. • 1: Enabled. Restricted is displayed.
LOG_CATEGORY	Null	Specifies a list of categories of events to be logged through syslog and locally. This parameter must be specified to log events below the Error level. The list can contain up to 255 characters. Category names are separated by commas without any intervening spaces.
LOG_DIALED_DIGITS	1	Specifies if the call log will contain digits dialed by a user or information about a remote party when the user dials a FAC code. The FAC code is identified by * or # entered as a first character. Value Operation: • 0: Allow dialed FAC code to be replaced with a remote party number in the call history • 1: Dialed digits are logged in call history exactly as they were entered by the user (default).
LOGSRVR	Null	Specifies one address for a syslog server in dotted-decimal formatl (IPv4), colon-hex format (IPv6, if supported), or DNS name format.

Table continues…

Parameter name	Default value	Description
		The value can contain 0 to 255 characters.
M		
MATCHTYPE	0	Specifies how an incoming or outgoing phone number is compared with the contacts on the phone to display the contact name. 0: Displays the contact name if all the digits match. 1: Displays the contact name if all the digits of the shorter number match with the right-most digits of the longer number. For example, a 5-digit extension number can be matched with the 8-digit phone number saved in the contacts. 2: Displays the contact name if 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. 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. Value operation: • 4: IPv4 • 6: IPv6 • 46: Prefer IPv4 over IPv6 • 64: Prefer IPv6 over IPv4
MEDIA_NEG_PREFERENCE	0	Specifies the address family preference used by a dual mode answer in non-Avaya environment.

Table continues…

Parameter name	Default value	Description
		This parameter is not applicable for single mode phones. Value operation: • 0: Remote or offerer's preference • 1: Local
MEDIA_PRESERVATION	1	Supports media preservation when ENABLE_IPOFFICE is set to 2. Value operation: • 0: Phone tries to preserve a call for a duration specified by PRESERVED_CALL_DURATION settings parameter. • 1: Phone does not preserve a call. As soon as the phone detects link failure to IP Office, the phone drops a call and makes re-registration attempt.
MEDIAENCRYPTION	9	Specifies which media encryption (SRTP) options is supported. 3 options are supported in a comma-separated list. Options must match to those specified in CM IP-codec-set form. • 1: aescm128-hmac80 • 2: aescm128-hmac32 • 3: aescm128-hmac80-unauth • 4: aescm128-hmac32-unauth • 5: aescm128-hmac80-unenc • 6: aescm128-hmac32-unenc • 7: aescm128-hmac80-unenc-unauth • 8: aescm128-hmac32-unenc-unauth • 9: none (default) • 10: aescm256-hmac80 • 11: aescm256-hmac32 The list of media encryption options is ordered from high (left) to the low

Table continues…

Parameter name	Default value	Description
		(right) options. The phone publishs this list in the SDP-OFFER or chooses from SDP-OFFER list according to the list order defined in MEDIAENCRYPTION. Avaya Aura® Communication Manager has the capability to change the list order in the SDP-OFFER (for audio only) when the SDP-OFFER is pass through. **Note:** You should not use unauthenticated media encryption (SRTP) files.
MLPP_MAX_PREC_LEVEL	1	Specifies the maximum allowed precedence level for the user. Value Operation: • 1: Routine • 2: Priority • 3: Immediate • 4: Flash • 5: Flash Override
MLPP_NET_DOMAIN	Null	Specifies the MLPP network domain. Value Operation: • Null: No domain configured • DSN: DSN network. • UC: UC network.
MSGNUM		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. **Note:** This parameter is applicable in Avaya Aura environment. In case of IP Office and third

Table continues…

Parameter name	Default value	Description
		party environment, use the parameter PSTN_VM_NUM.
MUTE_ON_REMOTE_OFF_HOOK	0	Controls the speakerphone muting for a remote-initiated (a shared control or OOD-REFER) speakerphone off-hook. Value Operation: • 0: The speakerphone is unmuted. • 1: The speakerphone is muted. 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 Manageror Avaya Aura® Communication Manager (SAT) administrative interfaces. **Note:** This parameter is set to 0 in IP Office environment.
MYCERTCAID	CAIdentifier	Specifies an identifier for the CA certificate with which the SCEP certificate request is to be signed, if the server hosts multiple Certificate Authorities. The value can contain zero to 255 ASCII characters. 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. The value must be a string that contains either $SERIALNO" (which

Table continues…

Parameter name	Default value	Description
		will be replaced by the phone's serial number) or $MACADDR (which will be replaced by the phone's MAC address), but it can contain other characters as well, including spaces. The value can contain eight ($MACADDR) to 255 characters.
MYCERTDN	Null	Specifies the part the SUBJECT of an SCEP certificate request that is common for all phones. The value must begin with a / and can include Organizational Unit, Organization, Location, State and Country. The value can contain Zero to 255 ASCII characters. **Note:** / must used as a separator between components. Commas do not work with some servers
MYCERTKEYLEN	2048	Specifies the bit length of the public and private keys generated for the SCEP certificate request. The value is a 4 ASCII numeric digits. The phone supports only value 2048.
MYCERTRENEW	90	Specifies the percentage of the identity certificate's validity interval after which renewal procedure is initiated. Valid values are 1 through 99.
MYCERTURL	Null	Specifies the URL of the SCEP server for obtaining an identity certificate. The URL can be HTTP or HTTPS. The valid values can range from Zero to 255 ASCII characters.
MYCERTWAIT	1	Specifies the phone's behavior if the SCEP server indicates that the

Table continues…

Parameter name	Default value	Description
		certificate request is pending for manual approval. Value Operation: • 0: Poll the SCEP server periodically in the background. • 1: Wait until a certificate is received or the request is rejected.
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. Valid values are 1 through 60.
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. Value operation: • 0: Certificate is considered to be revoked if the certificate revocation status is unknown. TLS connection will be closed. • 1: Certificate revocation operation will accept certificates for which the certificate revocation status is unknown.
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. Valid range is from 60 to 10080

Table continues…

Parameter name	Default value	Description
OCSP_ENABLED	0	Specifies that OCSP is used to check the revocation status of the certificates. Value operation: • 0: Disabled. Certificate revocation checking is not performed. • 1: Enabled. Certificate revocation checking is performed.
OCSP_HASH_ALGORITHM	0	Specifies the hashing algorithm for OCSP request. Value operation: • 0: SHA1 hash algorithm • 1: SHA256 hash algorithm
OCSP_NONCE	1	Specifies whether a nonce is added in OCSP requests and expected in OCSP responses. Value operation: • 0: Not added to OCSP request. • 1: Added to OCSP request.
OCSP_TRUSTCERTS		Specifies a comma separated list of OCSP trusted certificates that are used as OCSP signing authority for checking the revocation status of the certificate. This applies to when the OCSP responder is using a different CA. Spaces are not permitted in this parameter.
OCSP_URI	Null	Specifies the URI of an OCSP responder. The URI can be an IP address or hostname. Valid values contain 0 to 255 ASCII characters, zero or one URI.
OCSP_URI_PREF	1	Specifies the preferred URI for use in an OCSP request when more than one source is available. Value operation: • 1: Use the OCSP_URI and then the OCSP field of the Authority Information Access (AIA) extension of the certificate.

Table continues…

Parameter name	Default value	Description
		• 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. Value operation: • 0: OCSP is not used. Always check with OCSP responder. • 1: OSCP cache caching is used.
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.
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. Valid values are 60 through 31536000 (one year). The default value is 86400 (one day).
P		
PHNCC	1	Specifies the country code for United States. The value is 1. Valid values 1 through 999.
PHNDPLENGTH	5	Specifies the internal extension number length. If your extension is 12345, and your dial plan length is 5. The maximum extension length is 13. This value must match the extension length set on your call server. Valid values are 3 through 13.

Table continues…

Parameter name	Default value	Description
PHNEMERGNUM	Null	Specifies an emergency phone number to be dialed if the associated button is selected. Valid values can contain up to 30 dialable characters (0 to 9, *, #).
PHNMOREEMERGNUMS	Null	Specifies list of emergency numbers separated by comma. Valid values may contain up to 30 dialable characters (0 to 9, *, #).
PHNIC	011	Specifies the international access code For the United States, the value is 011. Valid values are from 0 to 4 dialable characters (0-9,*,#).
PHNLAC		Phone's Local Area Code indicates the phone's local area code, which along with the parameter LOCAL_DIAL_AREA_CODE, allows users to dial local numbers with more flexibility. PHNLAC is a string representing the local area code the phone. **Note:** This parameter is supported when the phone is failed over.
PHNLD	1	Specifies the long distance access code Valid values are 0 through 9 and empty string. If long distance access code is not needed then set the parameter to null.
PHNLDLENGTH	10	Specifies the national phone number length. For example, 800-555-1111 has a length of 10. Valid values are 5 through 15.
PHNMUTEALERT_BLOCK	1	Specifies if the **Mute Alert** feature is blocked or unblocked.

Table continues…

Parameter name	Default value	Description
		Value Operation: • 0: Unblocked • 1: Blocked
PHNNUMOFSA	3	Specifies the number of session appearances the phone must support while operating in a non-Avaya environment. Valid values are 1 through 10.
PHNOL	9	Specifies the outside line access code. This is the number you press to make an outside call. Valid values are 0 to 2 dialable characters (0-9, *, #).
PHONE_LOCK_IDLETIME	0	Specifies the interval of idle time, in minutes, after which the phone will automatically lock. The phone will lock irrespective of the value of ENABLE_PHONE_LOCK.
PHY1STAT	1	Specifies the speed and duplex settings for the Ethernet line interface. Value Operation: • 1: auto-negotiate • 2: 10Mbps half-duplex • 3: 10Mbps full-duplex • 4: 100Mbps half-duplex • 5: 100Mbps full-duplex • 6: 1Gbps full-duplex, if supported by hardware, otherwise auto-negotiated
PHY2_AUTOMDIX_ENABLED	1	Specifies whether auto-MDIX is enabled on PHY2. Value Operation: • 0: auto-MDIX is disabled. • 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. Valid values are 0 through 7.
PHY2STAT	1	Specifies the speed and duplex settings for the secondary (PC) Ethernet interface. Value Operation: • 0: disabled • 1: auto-negotiate • 2: 10Mbps half-duplex • 3: 10Mbps full-duplex • 4: 100Mbps half-duplex • 5: 100Mbps full-duplex • 6: 1Gbps full-duplex, if supported by hardware, otherwise auto-negotiated
PHY2TAGS	0	Determines whether or not VLAN tags are stripped on Ethernet frames going out of the Computer (PC) port. Value Operation: • 0: Strip tags. VLAN tags are stripped from Ethernet frames leaving the computer (PC) port of the phone. • 1: Does not strip tags. VLAN tags are not stripped from Ethernet frames leaving the Computer (PC) port of the phone. **Note:** This parameter is configured through the settings file.
PHY2VLAN	0	Specifies the value of the 802.1Q VLAN ID that is used to identify network traffic going into and

Table continues…

Parameter name	Default value	Description
		coming out of the internal CPU of the phone. Valid values are 0 through 4094. **Note:** The parameter is configured through the following: • SET command in a settings file • LLDP
PKCS12_PASSWD_RETRY	3	Specifies the number of retries for entering PKCS12 file password. If user failed to enter the correct PKCS12 file password after PKCS12_PASSWD_RETRY retries, then the phone will continue the startup sequence without installation of PKCS12 file. Valid values are from 0 to 100. Value operation: • 0: No retry
PKCS12URL	Null	Specifies the URL to be used to download a PKCS #12 file containing an identity certificate and its private key. Valid values contain 0 to 255 ASCII characters, zero or one URL. The value can be a string that contains either $SERIALNO or $MACADDR, but it may contain other characters as well. If $MACADDR is added to the URL, then the PKCS12 filename on the file server includes MAC address without colons. PKCS12 file download is preferred over SCEP if PKCS12URL is defined.
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.

Table continues…

Parameter name	Default value	Description
		Value Operation: • 0: Stop ringback tone as soon as SDP is received. • 1: Continue ringback tone until RTP is received (default).
POE_CONS_SUPPORT		Enables power over Ethernet conservation mode. Value Operation: • 0: Power conservation mode is not supported. • 1: Power conservation mode is supported.
PRESENCE_ACL_CONFIRM	0	Specifies the handling of a Presence ACL update with pending watchers. Value Operation: • 0: Auto confirm. Automatically send a PUBLISH to allow presence monitoring (default). • 1: Ignore. Take no action This parameter is not supported in IP Office environment as presence is not supported.
PRESENCE_SERVER	Null	Specifies the address of the Presence server. This parameter is supported only for backward compatibility. The value of this parameter is used from PPM and not from the settings file. 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 . The time interval can be from 10 minutes to 120 minutes.

Table continues…

Parameter name	Default value	Description
PROCPSWD	27238	Specifies an access code to access the admin menu procedures. Valid values contain 0 through 7 ASCII numeric digits. The default value is 27238 unless indicated otherwise below. A null value implies that an access code is not required for access. **Note:** • 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. • For enhanced security, use ADMIN_PASSWORD instead of PROCPSWD.
PROCSTAT	0	Specifies an access code to access the admin menu procedures. Value Operation: • 0: Local procedures can be used (default). • 1: Local procedures cannot be used.
PROVIDE_CF_RINGTONE	0	Specifies if the call forward ringtone option is provided to the user. Value Operation: • 0: The call forward ringtone option is not provided (default). • 1: The call forward ringtone option is provided.
PROVIDE_EXCHANGE_CALENDAR	1	Specifies if menu items for exchange calendar are displayed.

Table continues…

Parameter name	Default value	Description
		Value Operation: • 0: Not displayed • 1: Displayed (default) **Note:** Avaya J139 IP Phone does not support Exchange integration feature.
PROVIDE_EXCHANGE_CONTACTS	1	Specifies if menu items for exchange contacts are displayed. Value Operation: • 0: Not displayed • 1: Displayed (default) **Note:** Avaya J139 IP Phone does not support Exchange integration feature.
PROVIDE_KEY_REPEAT_DELAY	0	Specifies how long a navigation button must be held down before it begins to auto-repeat, and if an option is provided by which the user can change this value. Value Operation: • 0: Default (500ms) with user option (default). • 1: Short (250ms) with user option. • 2: Long (1000ms) with user option. • 3: Very Long (2000ms) with user option. • 4: No Repeat with user option. • 5: Default (500ms) without user option. • 6: Short (250ms) without user option. • 7: Long (1000ms) without user option.

Table continues…

Parameter name	Default value	Description
		• 8: Very Long (2000ms) without user option. • 9: No Repeat without user option.
PROVIDE_LOGOUT		Specifies if user can log out from the phone. Value Operation: • 0: No • 1: Yes **Note:** This parameter is set to 0 in IP Office environment.
PROVIDE_NETWORKINFO_SCREEN		Specifies if the **Network Information** menu is displayed on the phone. Value Operation: • 0: No • 1: Yes
PROVIDE_OPTIONS_SCREEN		Specifies if **Options & Settings** menu is displayed on phone. Value Operation: • 0: No • 1: Yes
PROVIDE_TRANSFER_TYPE	0	Provides the call transfer type in 3rd party environments. Value 0 or 1.
PSTN_VM_NUM		Specifies the dialable string that is used to call into the messaging system. For example, when you press the **Message Waiting** button. **Note:** This parameter is supported when the phone is failed over.
PUSHCAP	0000	Controls the modes of individual push types. The value is a 3, 4 or 5 digit number, of which each digit controls

Table continues…

Parameter name	Default value	Description
		a push type and can have a value of 0, 1 or 2. Value Operation: • 0: Push requests are ejected for that push type. • 1: Only push requests with a mode of barge are accepted for that push type. • 2: Push requests with a mode of barge or normal are accepted for that push type. The Push types controlled by each digit (11111) are as follows: • ||||+- The rightmost digit controls top line Push requests. • |||+-- The next digit to the left controls display (WML browser) push requests. • ||+--- The next digit to the left controls receive audio push requests. • |+---- The next digit to the left controls transmit audio push requests. • +----- The next digit to the left controls phonexml push requests.
PUSHPORT	80	Specifies the TCP port number to be used by the HTTP server in the phone for push. Valid values are 80 through 65535.
Q		
QLEVEL_MIN	1	Specifies the minimum quality level for which a low local network quality indication will not be displayed. Value Operation: • 1: Never display icon (default) • 2: Packet loss is > 5% or round trip network delay is > 720ms or

Table continues…

Parameter name	Default value	Description
		jitter compensation delay is > 160ms. • 3: Packet loss is > 4% or round trip network delay is > 640ms or jitter compensation delay is > 140ms. • 4: Packet loss is > 3% or round trip network delay is > 560ms or jitter compensation delay is > 120ms. • 5: Packet loss is > 2% or round trip network delay is > 480ms or jitter compensation delay is > 100ms. • 6: Packet loss is > 1% or round trip network delay is > 400ms or jitter compensation delay is > 80ms.
R		
RDS_INITIAL_RETRY_ATTEMPTS	15	Specifies the number of retries after which the phone abandons its attempt to contact the PPM server. Valid values are 1 through 30.
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. 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. Valid values are 2 through 3600.
RECORDINGTONE	0	Specifies whether call recording tone is generated on active calls. Value Operation: • 0: Call recording tone is not generated (default).

Table continues…

Parameter name	Default value	Description
		• 1: Call recording tone is not generated.
RECORDINGTONE_INTERVAL	15	Specifies the number of seconds between call recording tones. Valid values are 1 through 60.
RECORDINGTONE_VOLUME	0	Specifies the volume of the call recording tone in 5dB steps. Value Operation: • 0: The tone volume is equal to the transmit audio level (default). • 1: The tone volume is 45dB below the transmit audio level. • 2: The tone volume is 40dB below the transmit audio level. • 3: The tone volume is 35dB below the transmit audio level. • 4: The tone volume is 30dB below the transmit audio level. • 5: The tone volume is 25dB below the transmit audio level. • 6: The tone volume is 20dB below the transmit audio level. • 7: The tone volume is 15dB below the transmit audio level. • 8: The tone volume is 10dB below the transmit audio level. • 9: The tone volume is 5dB below the transmit audio level. • 10: The tone volume is equal to the transmit audio level.
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 will try again after a randomly selected delay of 50% to 90% of the value of RECOVERYREGISTERWAIT.

Table continues…

Parameter name	Default value	Description
		Valid values are 10 through 36000.
REDIRECT_TONE	1	Specifies the tone to play when a call goes to coverage. Valid values are from 1 to 4.
REGISTERWAIT	900	Specifies the number of seconds between re-registrations with the current server. Valid values are from 30 to 86400.
REUSETIME	60	Specifies the number of seconds that the DHCP is attempted: • With a VLAN ID of zero. True when L2Q is set to 1. • Or with untagged frames. True if L2Q is set to 0 or 2. • And before reusing the IP address and the associated address information, that the phone had the last time it successfully registered with a call server. While reusing an address, DHCP enters the extended rebinding state described above for DHCPSTD. Valid values are 0 and 20 through 999. The default value is 60. A value of zero means that DHCP will try forever and there will be no reuse.
RINGTONES	Null	Specifies a list of display names and file names or URLs for a custom ring tone files to be downloaded and offered to users. The list can contain 0 to 1023 UTF-8 characters. The default value is null. Values are separated by commas without any intervening spaces. Each value consists of a display name followed by an equals sign followed by a file name or URL. Display names can contain spaces, but if any do, the entire list must be

Table continues…

Parameter name	Default value	Description
		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. Value Operation: • 0: Phone only tries to download ring tones with new display names. • 1: Phone checks for updated version of each ring tone file at startup.
RINGTONESTYLE	0	Specifies the style of ring tones that are offered to the user for personalized ringing when **Classic** is selected, as opposed to **Rich**. Value Operation: • 0: North American ring tones are offered (default). • 1: European ring tones are offered.
RTCP_XR	0	Specifies if VoIP Metrics Report Block as defined in RTP Control Protocol Extended Reports (RTCP XR) (RFC 3611) is sent as part of the RTCP packets to remote peer or to RTCP monitoring server. Value Operation: • 0: No • 1: Yes
RTCPCONT		Specifies if the sending of RTCP is enabled. Value Operation: • 0: No • 1: Yes

Table continues…

Parameter name	Default value	Description
RTCPMON	Null	Specifies the IP or DNS address for the RTCP monitor. You can set this parameter only if the environment is not an Avaya environment. The values can range from 0 through 255 characters.
RTCPMONPERIOD	5	Specifies the interval, in seconds, for sending out RTCP monitoring reports. Valid values are from 5 to 30 seconds.
RTCPMONPORT	5005	Specifies the RTCP monitor port number. You can set this parameter only if the environment is not an Avaya environment. The values can range from 0 through 65535. Default is 5005.
RTP_PORT_LOW		Specifies the lower limit of the UDP port range to be used by RTP or RTCP and SRTP or SRTCP connections. The values can range from 1024 through 65503.
RTP_PORT_RANGE		Specifies the range or number of UDP ports available for RTP or RTCP and SRTP or SRTCP connections This value is added to RTP_PORT_LOW to determine the upper limit of the UDP port range. The values can range from 32 through 64511.
S		
SCEPPASSWORD	$SERIALNO	Specifies the password to be included in the change password attribute of an SCEP certificate request. Values can contain 0 to 32 ASCII characters (50 ASCII characters. If the value contains $SERIALNO, it is replaced by the phone's serial

Table continues…

Parameter name	Default value	Description
		number. If the value contains $MACADDR, it is replaced by the phone's MAC address in hex. **Note:** • A password prompt is invoked when SCEP is set for identity certificate enrollment and the parameter value is empty. • This parameter must not be set in a file that is accessible on an enterprise network, and only in a restricted staging configuration.
SCREENSAVER_IMAGE	N/A	Specifies the screen saver images those can be loaded from the provisioning server. Maximum five custom images can be uploaded onto the phone. Only the .jpeg file format are supported and the maximum file size is 256KB. 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.
SCREENSAVER_IMAGE_SELECTABLE	1	Allows the end user to select and change the screen saver images. Value operation: • 0: End user can not select and change the screen saver images from the settings menu. • 1: End user can select and change the screen saver images from the settings menu.

Table continues…

Parameter name	Default value	Description
		Note: Only Avaya J169/J179 IP Phone supports this feature.
SCREENSAVERON	240 (4 hours)	Specifies the number of minutes of idle time after which the screen saver is displayed. If an image file is downloaded based on the LOGOS and CURRENT_LOGO parameter, it is used as the screen saver. Otherwise, the built-in Avaya one-X(TM) screen saver is used. Valid values are 0 through 999. The default value is 240 (4 hours). A value of 0 means that the screen saver will not be displayed automatically when the phone is idle.
SDPCAPNEG	1	Specifies if SDP capability negotiation is enabled. Value Operation: • 0: SDP capability negotiation is disabled. • 1: SDP capability negotiation is enabled.
SEND_DTMF_TYPE	2	Specifies if DTMF tones are sent in-band as regular audio, or out-of-band using RFC 2833 procedures. Value Operation: • 1: In-band • 2: Out-of-band
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.

Table continues…

Parameter name	Default value	Description
		Value operation: • 0: Periodic checking is disabled.
SHOW_LAST_EXTENSION	0	Specifies whether to display last extension after logout. Value Operation: • 0: To hide last extension after logout. • 1: To display the last extension after logout.
SIG	0	Specifies the type of software to be used by the phone by controlling which upgrade file is requested after a power-up or a reset. Value Operation: 0: Download the upgrade file for the same signaling protocol that is supported by the current software (default) 2: Download J100Supgrade.txt
SIG_PORT_LOW		Specifies the minimum port value for SIP signaling. (1024 -65503).
SIG_PORT_RANGE		Specifies the range or number of SIP signaling ports. This value is added to SIG_PORT_LOW to determine the upper limit of the SIP signaling port range (32-64511).
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. Value operation: • 4: IPv4 • 6: IPv6
SIMULTANEOUS_REGISTRATIONS	3	Specifies the number of Session Managers with which the phone simultaneously register. Valid values are 1, 2 or 3. The default value is 3.

Table continues…

Parameter name	Default value	Description
		Note: 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. Controller designator has the following format: `host[:port] [;transport=xxx]` where • `host` is an proxy address in dotted-decimal or DNS name format. In third-party call control setup, only DNS format is supported. • `[:port]` is an optional port number. • `[;transport=xxx]` is an optional transport type where `xxx` can be TLS, TCP, or UDP. For example, `SIP_CONTROLLER_LIST="10.138.251.56:5060;transport=tcp"`
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. Valid values are 0 to 255 characters in the dotted decimal or colon-hex format. The SIP Proxy list has the following format: `host[:port] [;transport=xxx]` where • `host` is IP addresses in dotted-decimal format or hex format. • `[:port]` is the port number. The default values are 5060 for TCP and 5061 for TLS.

Table continues…

Parameter name	Default value	Description
		• `[;transport=xxx]` is the transport type and `xxx` is either TLS or TCP. The default value is TLS. For example, `SIP_CONTROLLER_LIST_2="10.16.26.88:5060;transport=tcp"`
SIPCONFERENCECONTINUE	0	Specifies if a conference call continues after the host hangs up. Value Operation: • 0: Drop all parties. • 1: Continue conference **Note:** This parameter is set to 1 in IP Office environment.
SIPDOMAIN	Null	Specifies the domain name to be used during SIP registration. The value can contain 0 to 255 characters. The default value is null.
SIPPORT	5060	Specifies the port the phone opens to receive SIP signaling messages. 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. Value Operation: • Alternate: Only a single registration is attempted and maintained. • Simultaneous: Simultaneous registrations is attempted and maintained with all available controllers.
SKILLSCREENTIME	5	Specifies the duration, in seconds, that the **Skills** screen is displayed.

Table continues…

Parameter name	Default value	Description
		Valid values are 0 through 60. The default value is 5. A value of 0 means that the **Skills** screen in not removed automatically when the agent logs in.
SLMCAP	0	Specifies if the SLA Monitor agent is enabled for packet capture. Value Operation: • 0: Disabled (default) • 1: Enabled and payloads are removed from RTP packets • 2: Enabled and payloads are included in RTP packets • 3: Controlled from admin menu - Allows you to enable or disable of RTP packets capture using local admin procedures.
SLMCTRL	0	Specifies whether the SLA Monitor agent is enabled for phone control. Value Operation: • 0: Disabled • 1: Enabled • 2: Controlled from admin menu.
SLMPERF	0	Specifies whether the SLA Monitor agent is enabled for phone performance monitoring. Value Operation: • 0: Disabled • 1: Enabled
SLMPORT	50011	Specifies the UDP port that will be opened by the SLA Monitor agent to receive discovery and test request messages. Valid values are 6000 through 65535. The default value is 50011.

Table continues…

Parameter name	Default value	Description
		Note: If default port is not used, both the SLA Mon agent and the server must be configured with the same port. This parameter impacts the phone's SLA Mon agent configuration. A corresponding configuration must also be made on the SLA Mon server `agentcom-slamon.conf` file.
SLMSRVR		Specifies the IP address and the port number of the SLA Mon server in the aaa.bbb.ccc.ddd:n format. Set the IP address of the SLA Mon server in the aaa.bbb.ccc.ddd format to restrict the registration of agents only to that server. Specifying a port number is optional. If you do not specify a port number, the system takes 50011 as the default port. If the value of the port number is 0, than any port number is acceptable. The IP address must be in the dotted decimal format, optionally followed by a colon and an integer port number from 0 to 65535. 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. **Note:** If default port is not used, both the SLA Mon agent and server must be configured with the same port. SLMSRVR impacts the phone's SLA Mon agent configuration. A corresponding configuration must also be made on the SLA Mon server `agentcom-slamon.conf` file

Table continues…

Parameter name	Default value	Description
SLMSTAT	0	Specifies if the SLA Monitor agent is enabled or not. Value Operation: • 0: Disabled • 1: Enabled
SNMPADD	Null	Specifies a list of source IP addresses from which SNMP query messages will be accepted and processed. Addresses can be in dotted-decimal format (IPv4), colon-hex format (IPv6, if supported), or DNS name format, separated by commas without any intervening spaces. The list can contain up to 255 characters. The default value is null.
SNMPSTRING	Null	Specifies a security string that must be included in SNMP query messages for the query to be processed. Valid values contain 0 through 32 ASCII alphanumeric characters. The default value is null. Null disables SNMP.
SNTP_SYNC_INTERVAL	1440 minutes	Specifies the time interval, in minutes, during which the phone will attempt 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. Addresses can be in dotted-decimal or DNS name format, separated by commas without any intervening spaces. The list can contain up to 255 characters.

Table continues…

Parameter name	Default value	Description
SOFTKEY_CONFIGURATION	0,1,2	Specifies which feature will show up on which softkey on the Avaya J129 IP Phonescreens. The features are defined as follows: • 0 = Redial • 1 = Contacts • 2 = Emergency • 3 = Recents • 4 = Voicemail
SPEAKERSTAT	2	Specifies the operation of the speakerphone. Value Operation: • 0: Speakerphone disabled • 1: One-way speaker (also called monitor) enabled. • 2: Full (two-way) speakerphone enabled. **Note:** This parameter is not supported on Avaya J129 IP Phone.
SSH_ALLOWED	2	Specifies if SSH is supported. Value Operation: • 0: Disabled • 1: Enabled • 2: Configured using local admin procedure. When this mode is configured, then by default the SSH server is disabled.
SSH_BANNER_FILE	Null	Specifies the file name or URL for a custom SSH banner file. If the value is null, english banner is used for SSH. The value can contain 0 to 255 characters.

Table continues…

Parameter name	Default value	Description
SSH_IDLE_TIMEOUT	10	Specifies the idle time in minutes after which an SSH connection is terminated Valid values are 0 through 32767. A value of 0 means that the connection will not be terminated.
SUBSCRIBE_LIST_NON_AVAYA		Specifies comma separated list of event packages to subscribe to after registration. Possible values are: reg, dialog, mwi, ccs, message-summary which is identical to mwi, avaya-ccs-profile which is identical to ccs. The values are case insensitive. For IPO the recommended value shall be reg, message-summary, avaya-ccs-profile.
SUBSCRIBE_SECURITY		Specifies the use of SIP or SIPS for subscriptions. Value Operation: • 0: The phone uses SIP for both the request URI and the contactheader regardless of whether SRTP is enabled. • 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. • 2: SES or PPM does not show a FS-phoneData FeatureName with a Feature Version of 2 in the response to the getHomeCapabilities request. For IP office environment, the applicable values are 0 and 1.
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

Table continues…

Parameter name	Default value	Description
		the RTP or SRTP datagrams of that endpoint. Value Operation: • 0: Ignore the UDP source port number in received RTP/SRTP datagrams. • 1: Discard received RTP/SRTP datagrams if their UDP Source Port number does not match the UDP Destination Port number that the phone includes in RTP/SRTP datagrams intended for that phone.
SYSTEM_LANGUAGE		Contains the name of the default system language file used in the phone. The filename should be one of the files listed in the LANGUAGES parameter. If no filename is specified, or if the filename does not match one of the LANGUAGES values, the phone uses the built-in English text strings. Valid values range from 0 through 32 ASCII characters. Filename must end in .xml
T		
TCP_KEEP_ALIVE_INTERVAL	10	Specifies the number of seconds that the telephone waits before re-transmitting a TCP keep-alive (TCP ACK) message. Valid values are from 5 through 60.
TCP_KEEP_ALIVE_STATUS	1	Specifies if the phone sends TCP keep alive messages. Value Operation: • 0: Keep-alive messages are not sent. • 1: Keep-alive messages are sent (default).

Table continues…

Parameter name	Default value	Description
TCP_KEEP_ALIVE_TIME	60	Specifies the number of seconds that the telephone waits before sending out a TCP keep-alive (TCP ACK) message. Valid values are from 10 through 3600
TEAM_BUTTON_REDIRECT_INDICATION	0	Specifies if the redirection indication must be shown on a team button on the monitored station, if it is not a redirect destination of the monitored station. Value Operation: • 0: Disabled. The redirect indication is shown only on a monitoring station which is redirection destination. • 1: Enabled. The redirection indication is displayed on all monitoring stations. **Note:** Avaya J139 IP Phone does not support this feature.
TEAM_BUTTON_RING_TYPE	1	Specifies the alerting pattern to use for team buttons. Valid values are 1 through 8. The default value is 1. **Note:** Avaya J139 IP Phone does not support Team Button feature.
TIMEFORMAT		Specifies the format for time displayed in the phone. The TIMEFORMAT parameter is used when the phone fails to get time format from the PPM. Value Operation: • 0: AM or PM format. • 1: 24 hour format

Table continues…

Parameter name	Default value	Description
TLS_VERSION	0	Specifies the TLS version used for all TLS connections (except SLA monitor agent) Value Operation 0: TLS versions 1.0 and 1.2 are supported. 1: TLS version 1.2 only is supported.
TLSDIR		Specifies the HTTPS Server Directory Path. Valid values can contain 0 to 127 ASCII characters, without any spaces.
TLSPORT	443	Specifies the TCP port used for HTTPS file downloads from non-Avaya servers. Valid values are from 0 to 65535.
TLSSRVR		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. Value Operation: • 0: Identity matching is not performed. • 1: The certificate is trusted only if the identity used to connect to the server matches the certificate identity, as per Section 3.1 of RFC 2818. For SIP-TLS connections, an additional check is performed to validate the SIP domain identified in the certificate, as per RFC 5922. The

Table continues…

Parameter name	Default value	Description
		parameter is configured through the `46xxsettings.txt` file.
TPSLIST	Null	Specifies a list of URI authority components (optionally, including scheme and path components) to be trusted. A URI received in a push request is only used to obtain push content, if it matches one of these values. The list can contain up to 255 characters. Values are separated by commas without any intervening spaces. If the value of TPSLIST is null, push is disabled.
TRUSTCERTS		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
U		
USE_EXCHANGE_CALENDAR	0	Specifies whether the Calendar synchronizes with the Microsoft Exchange. Value operation: • 0: To disable synchronization. • 1: To enable synchronization.
USER_STORE_URI		Specifies the URI path of IP Office for storing user data. **Note:** If the value of this parameter is set to null, then the addition, deletion, and modification of **Contacts** is disabled.
UUIDISPLAYTIME	10	Specifies the duration, in seconds, that the **UUI Information** screen is be displayed. Valid values are 5 through 60.

Table continues…

Parameter name	Default value	Description
V		
VLANSEPMODE	1	Specifies whether full VLAN separation will be enabled by the built-in Ethernet switch while the telephone is tagging frames with a non-zero VLAN ID. PHY2PRIO is not supported when VLANSEPMODE is 1. Value operation: • 0: Disabled • 1: Enabled **Note:** This parameter is configured through the settings file.
VLANTEST	60	Specifies the number of seconds that the phone waits prior to failing back to a different VLAN ID if no response is received from the DHCP server. Valid values are 0 through 999. A value of zero means that DHCP tries with a non-zero VLAN ID forever. **Note:** This parameter is configured through: • Settings file • A name equal to value pair in DHCPACK message
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. If there is no change to volume levels, there will be no backup to PPM service. Valid values are 2 through 900. The default value is 2.

Table continues…

Parameter name	Default value	Description
W		
WAIT_FOR_INVITE_RESPONSE_TIMEOUT	60	Specifies the maximum number of seconds that the phone waits for another response after receiving a SIP 100 Trying response. Valid values are 30 through 180.
WAIT_FOR_REGISTRATION_TIMER	32	Specifies the number of seconds that the phone waits for a response to a REGISTER request. If no response message is received within this time, registration will be retried based on the value of RECOVERYREGISTERWAIT. Valid values are 4 through 3600.
WAIT_FOR_UNREGISTRATION_TIMER	32	Specifies the number of seconds the phone waits before assuming that an un-registration request is complete. Un-registration includes termination of registration and all active dialogs. Valid values are 4 through 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. The value can contain 0 to 255 characters.
WBCSTAT	1	Specifies whether a wideband codec indication is displayed when a wideband codec is used. Value Operation: • 0: Disabled • 1: Enabled
WEB_ADMIN_PASSWORD	27238	Specifies the password to access the phone through a web browser as an administrator.

Table continues…

Parameter name	Default value	Description
		The value set from the web server interface has a higher priority than that of the Settings file. If the Web admin password is changed using the web server, then the web admin password set through settings file is not used until either the web admin password is set to default through the phone admin menu or the phone is reset to default. Valid values are from 8 to 31 alphanumeric characters including upper, lower and special characters.
WEB_HTTP_PORT	80	Specifies the port on which the Web Server running on the phone will be accessed using HTTP. Valid values are 0, 80, 1024 to 65535.
WEB_HTTPS_PORT	443	Specifies the port on which the Web Server running on the phone will be accessed using HTTPS. Valid values are 443, 1024 to 65535.
WEBSERVER_ON_HTTP	0	Specifies whether HTTP access to the web server is enabled or disabled. Value operation: • 0: Web Server is not accessible through HTTP. • 1: Web Server is accessible through HTTP.

Chapter 14: 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.	For people who want to gain a high-level understanding of the Avaya Aura® Session Manager features, functions, capacities, and limitations.
Avaya IP Office™ Platform Feature Description	See information about the feature descriptions.	For people who perform system administration tasks.
Avaya IP Office™ Platform Solution Description	See information about how the products and services that interoperate with this solution.	For 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.	For people who install, configure, and verify Avaya Aura® Session Manager on Avaya Aura® System Platform.
Upgrading Avaya Aura® Session Manager	See upgrading checklists and procedures.	For 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.	For people who install, configure, and verify Avaya Aura®

Table continues…

Title	Use this document to:	Audience
		System Manager on Avaya Aura® System Platform at a customer site.
Avaya IP Office™ Platform SIP Telephone Installation Notes	See the installation procedures and initial administration information for IP Office SIP telephone devices.	For people who install, configure and verify SIP telephone devices on IP Office.
Administering		
Administering Avaya Aura® Session Manager	See information about how to perform Avaya Aura® Session Manager administration tasks including how to use management tools, how to manage data and security, an how to perform periodic maintenance tasks.	For people who perform Avaya Aura® Session Manager system administration tasks.
Administering Avaya Aura® System Manager	See information about how to perform Avaya Aura® System Manager administration tasks including how to use management tools, how to manage data and security, an how to perform periodic maintenance tasks.	For 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	For 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.	For people who perfrom IP Office Web Manager administration tasks.
Maintaining		
Maintaining Avaya Aura® Session Manager	See information about the maintenance tasks for Avaya Aura® Session Manager.	For people who maintain Avaya Aura® Session Manager.
Troubleshooting Avaya Aura® Session Manager	See information for troubleshooting Avaya Aura® Session Manager, resolving alarms, replacing hardware, and alarm codes and event ID descriptions.	For people who troubleshoot Avaya Aura® Session Manager.
Using Avaya IP Office™ Platform System Status Application	See information about the maintenance tasks for System Status Application.	For people who maintain System Status Application.
Using Avaya IP Office™ Platform System Monitor	See information about the maintenance tasks for SysMonitor.	For 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 an appropriate release number.
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 displays the documents only from the selected category.
7. Click **Enter**.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com/.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open https://support.avaya.com/.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **My Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.

  - Add content from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive content that others have shared with you.

- Add yourself as a watcher by using the **Watch** icon ().

  Navigate to the **My Content** > **Watch list** menu, and do the following:

  - Set how frequently you want to be notified, starting from every day to every 60 days.
  - 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 portal.
- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

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.

Procedure

- 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` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- 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 the name of a topic to see the available list of videos posted on the website.

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.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W