Installing and Administering Avaya J129 IP Phone

Release 1.0
Issue 1
December 2016

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. 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 Designated Processor that hosts 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 on a number of Designated Processors up to the number indicated in the order. 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. Note that 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 G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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 device complies with Industry Canada's RF radiation exposure limits set forth for the general population (uncontrolled environment) and must not be co-located or operated in conjunction with any other antenna or transmitter.

Cet appareil est conforme aux limites d'exposition aux rayonnements RF d'Industrie Canada énoncés dans la population générale (environnement non contrôlé) et ne doivent pas être co-situés ou exploités conjointement avec une autre antenne ou émetteur.

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.

Class B Part 15 Statement

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.

EU Countries

This device complies with the essential requirements and other relevant provisions of Directive 1999/5/EC. A copy of the Declaration may be obtained from http://support.avaya.com or Avaya Inc., 211 Mt. Airy Road, Basking Ridge, NJ 07920 USA.

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.
  - Limit the power to the device over telecommunications wiring to 36-57 volt DC or ≤ 1.3 ampere DC.

Trademarks

Contents

Chapter 1: Introduction

Purpose

This document provides information about how to perform system administration tasks including how to use management tools, how to manage data and security, and how to perform periodic maintenance tasks.

Intended audience

This document is intended for people who perform the product or solution system administration tasks.

Chapter 2: Avaya J129 IP Phone

The Avaya J129 IP Phone are SIP-based IP phones for unified communications. Avaya J129 IP Phone support a single line with two call appearances on a dual line display.

Specifications

Specification	Category	Description
Hardware	Display	A graphical LCD display with a display resolution of 128 x 32 px.
	Audio	Supported audio codecs are: • G.711 A-law/mu-law • G.726 A • G.729 • G.729 A • G.729 AB • G.722 • OPUS
	Softkeys	Three buttons located below the display.
	Switch hook	Magnetic switch-hook.
	Handset	Wired handset
	Headset	No headset support on Avaya J129 IP Phone.
	Speaker	Hands-free operation
	Physical buttons and LEDs	• Dialpad: 0–9, *, # • Volume: **+** and **—** buttons • Mute button • Hold button • Phone button • Speaker button

Table continues…

Specification	Category	Description
		• Main menu • Back button • Beacon LED • Navigation arrows and OK button
	Network connectors	• RJ45 primary Ethernet (10/100 Mbps) network port. • RJ45 secondary Ethernet (10/100 Mbps) computer port.
Power	Ethernet	• IEEE 802.3at • Single Port PoE injector (SPPoE)

Physical layout

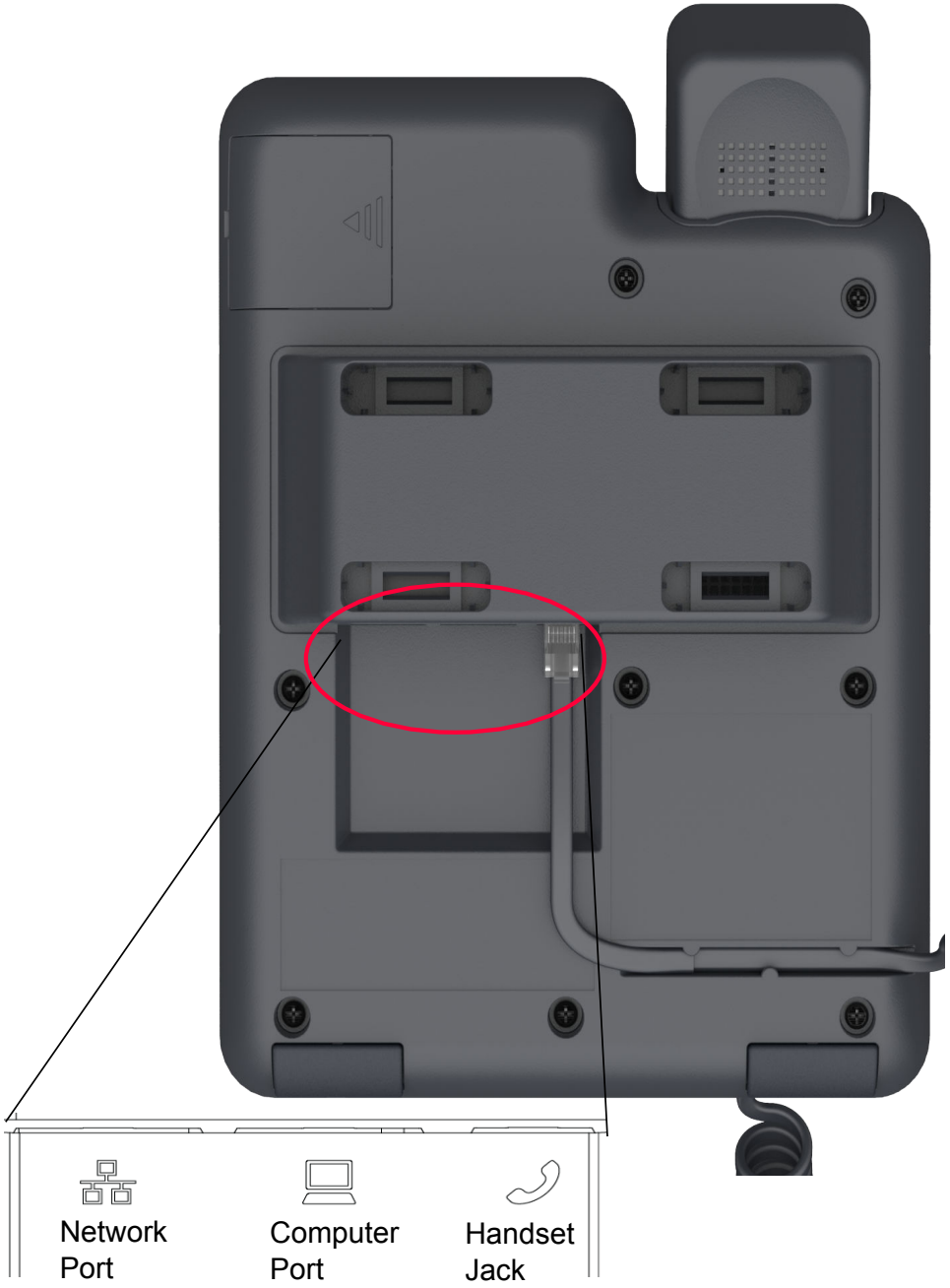
Callout number	Name	Button Icon	Description
1	Beacon LED	N/A	The beacon LED flashes a red light to the upper-right corner of the phone, which indicates that you have a voice mail, an incoming call or you are on a call using the hands free speaker capability.
2	Phone display	N/A	The phone displays the call information in this area, such as the extension, caller information, and missed calls. **Note:** • If there are three dots after a text, use the right and left arrow keys to scroll through the text. • If there is a scroll bar or line indicator at the right of the phone display, use the up and down arrow keys to scroll up and down.
3	Softkeys	N/A	The softkeys selects the action that is displayed in the softkey section of the phone display. The softkeys are context sensitive.
4	Navigation arrows and OK		The **OK** button performs the action of selecting the function assigned to the left most soft key function. The navigation arrows performs the action of scrolling through various sections of the phone display.
5	Phone		Press the **Phone** button to move to the Phone screen.
6	Back		Press the **Back** button to cancel the current action and return to the previous menu.
7	Speaker		Press the **Speaker** button to use the speakerphone. To take the call off the speakerphone, lift the handset.
8	Main Menu		Press the **Main Menu** button to access the menu options and other phone settings.
9	Hold		Press **Hold** button to place the call on hold.

Table continues…

Callout number	Name	Button Icon	Description
			To resume the call, press the **Resume** softkey.
10	Volume		If you press or on the **Volume** button on an active call, the phone increases or decreases the volume of your handset, or speaker accordingly. When you are not on an active call, pressing these buttons adjusts the ringer volume.
11	Mute		Press the **Mute** button to mute a call in progress. To unmute the call, press the **Mute** button again.

Connection jacks

The following image illustrates the connection jacks that are present on the back panel of Avaya J129 IP Phone models. The image schematically describes which device to connect in which jack.


Network
Port
Computer
Port
Handset
Jack

Chapter 3: Initial setup and connectivity

Avaya J129 IP Phone deployment in the Avaya Aura® environment

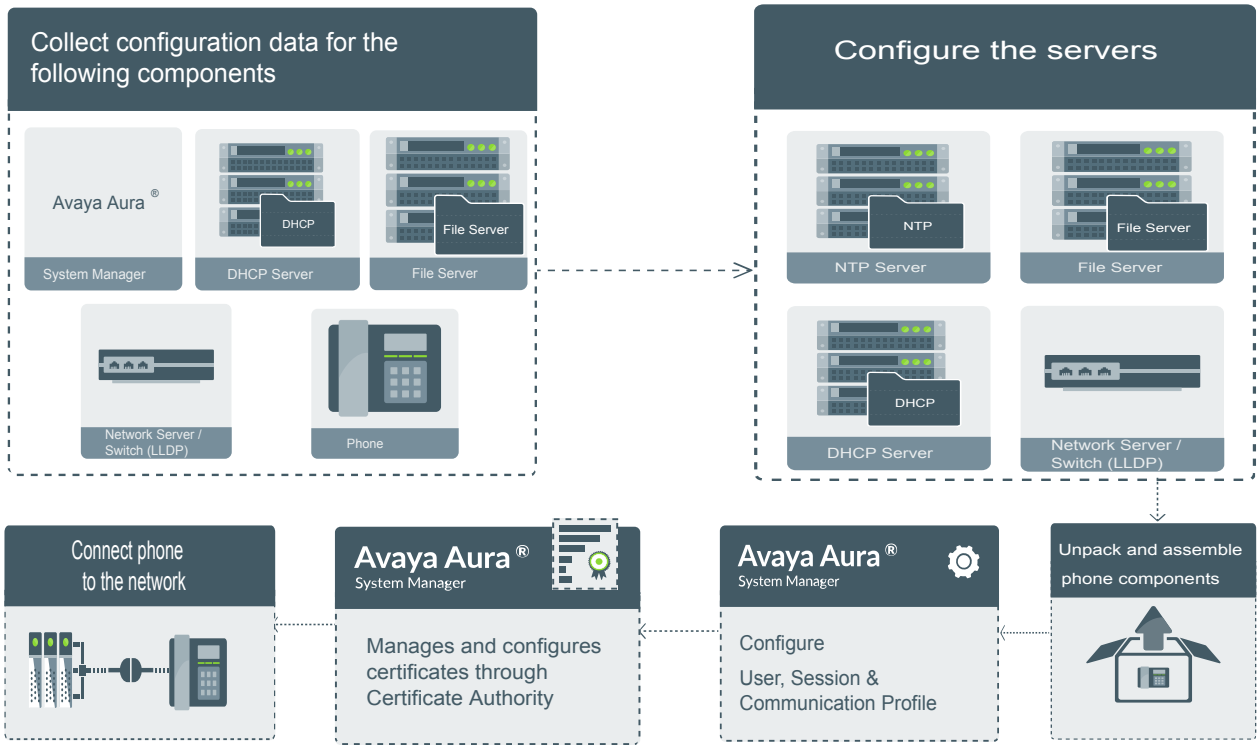


Figure 1: Avaya J129 IP Phone deployment in the Avaya Aura® environment

Avaya J129 IP Phone deployment in IP Office

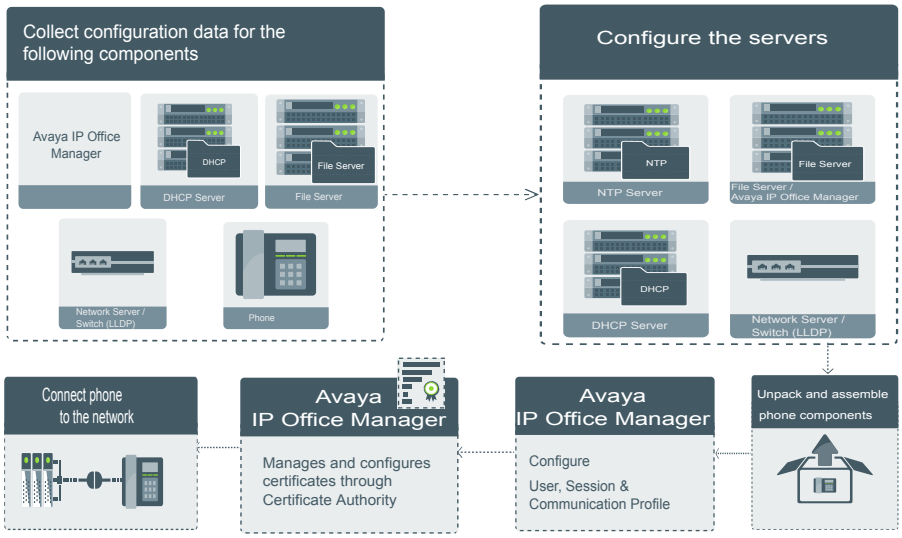


Figure 2: Avaya J129 IP Phone deployment IP Office

Installation checklist

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

No.	Task	Reference	✔
1	Check the prerequisites	Prerequisites on page 19	
2	Gather preinstallation data	Preinstallation data gathering on page 20	
3	Configure the servers	Server Configuration	
4	Configure the settings file only for Avaya Aura® environment	List of configuration parameters on page 85	
5	Configure the upgrade file	Device upgrade overview on page 68	
6	Create users on Avaya Aura® System Manager and IP Office	*Administering Avaya Aura® Avaya Aura® System Manager for Release 7.1*	
7	Administer the VLAN	VLAN overview on page 33	
8	Install the phone	Installing the phone on page 24	

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	✔	✔	—	—	✔

Precedence of the methods

Most of the parameters are configurable 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 admin menu of the phone.
2. Avaya Aura® System Manager and IP Office.
3. Settings file.
4. DHCP.
5. 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 Settings file are removed, or are not used, they reset to their default value.

Prerequisites

Check the prerequisites to ensure that you have the required software and hardware before you install the Avaya J129 IP Phone.

Software requirements

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.
- Avaya Aura® Presence Services 6.2.4 or later.
- Avaya Aura® Session Border Controller 7.0 and 7.0.1.
- Avaya Aura® Media Server 7.7.0.334.
- A DHCP server for providing dynamic IP addresses to the Avaya J129 IP Phone.
- A file server, an HTTP, HTTPS, or the Avaya Utility server for downloading the software distribution package and the settings file.

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

Note:

Avaya J129 IP Phone can be deployed on IP Office 10.0 SP2 onwards. For more information about the prerequisites, see *Avaya IP Office™ Platform SIP Telephone Installation Notes*.

Hardware requirements

Ensure that the LAN uses:

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

Preinstallation data gathering

Populate values in the following table for the data that you would require at different stages of installation.

Data for	Field	Value	Notes
System Manager User Profile			
Identity tab			
	Login Name		
	Localized Display Name		
	Endpoint Display Name		
	Language Preference		
	Time Zone		
Presence Profile			
	System		
	IM Gateway SIP Entity		
	Publish Presence with AES collector		
Communication Profile tab			
Communication Profile section			
	Communication Profile Password		
Session Manager Profile section			
	Primary Session manager		
	Secondary Session Manager		
	Survivability Server		
CM Endpoint Profile section			

Table continues…

Data for	Field	Value	Notes
	System		
	Profile Type		
	Use Existing Endpoints		
	Extension		
	Endpoint Template		
	Voice Mail Number		
Messaging Profile section			Optional
	System		
	Mailbox Number		
	Template		
	Password		
SIP settings			For registering phones.
	SIP controller list		
	SIP domain		
File server address			To download the software distribution package and the settings file.
	HTTP server or TLS server		Set the appropriate file server address in the `46xxsettings.txt file`, LLDP and DHCP.

Note:

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

Downloading and saving the software

Before you begin

Ensure that your file server is set up.

Procedure

1. Go to the Avaya Support website.
2. In the **Enter Your Product Here** field, enter Avaya J129 IP Phone.
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

Manual upgrade on page 69
Software distribution package on page 22

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 J129 IP Phone 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 J129 IP Phone 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

Downloading and saving the software on page 21

Configuring the Settings file

About this task

Use this procedure to modify the Settings file with appropriate values to provision the device configuration parameters.

Note:

This procedure applies to Avaya Aura® environment only. In IP Office the Settings file is auto generated and cannot be modified.

Procedure

1. On the file server, go to the location where you downloaded the `46xxsettings.txt` Settings file.
2. Open the Settings file in a text editor.
3. Set the required parameters.

   Note:

   Avaya J129 IP Phone parameters stored for a particular user are not reflected in other phones, for example, 9600 Series IP Deskphones, even if the SIP user is the same.
4. Save the Settings file.

Related links

List of configuration parameters on page 85

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 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.
   b. 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.
   c. The phone verifies the VLAN ID, and starts tagging the data and voice packets accordingly.
   d. The phone checks for LLDP messages and re-checks VLAN status and tagging.

      If LLDP has changed the values of L2Q or L2QVLAN, the phone resets to obtain a new IP address.
   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?		
2	Are you able to make a call from the phone?		
3	Are you able to modify the phone's Settings file parameters and end user settings.	List of configuration parameters on page 85	
4	Are you able to upgrade your phone?	Device upgrade process on page 68	
5	For security considerations, have you configured the phone setup with TLS signaling? Have you installed the appropriate private network authentication certificates?		
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:

- *Avana IP Office™ Platform Solution Description*
- *Avana IP Office™ Platform Feature Description*

Chapter 4: 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
- Device interface
- Settings file

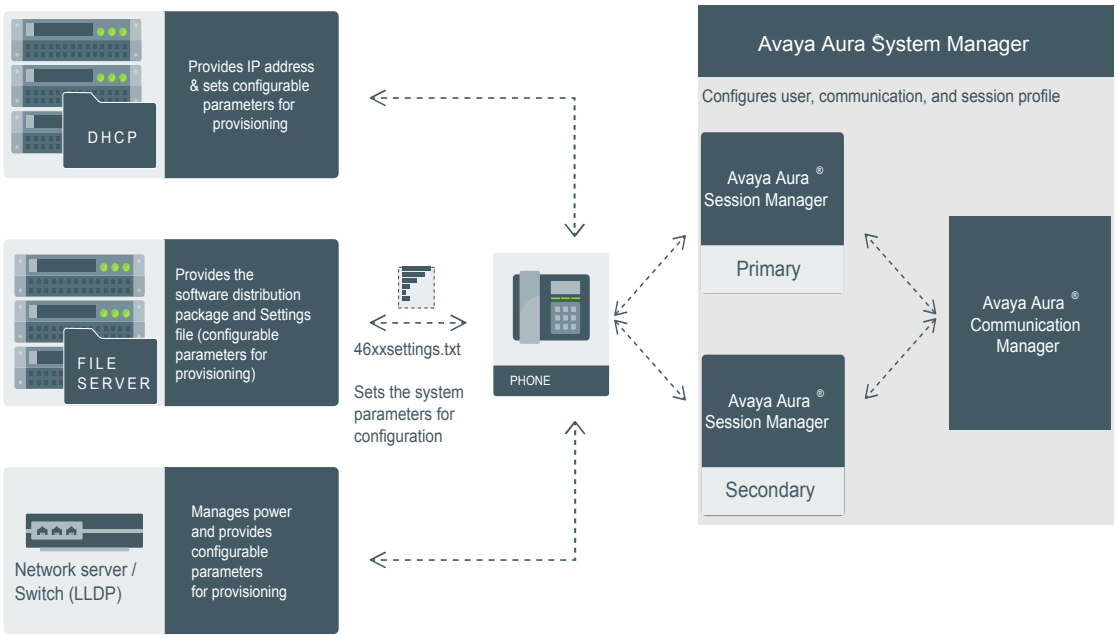


Figure 3: Setup in Avaya Aura® environment

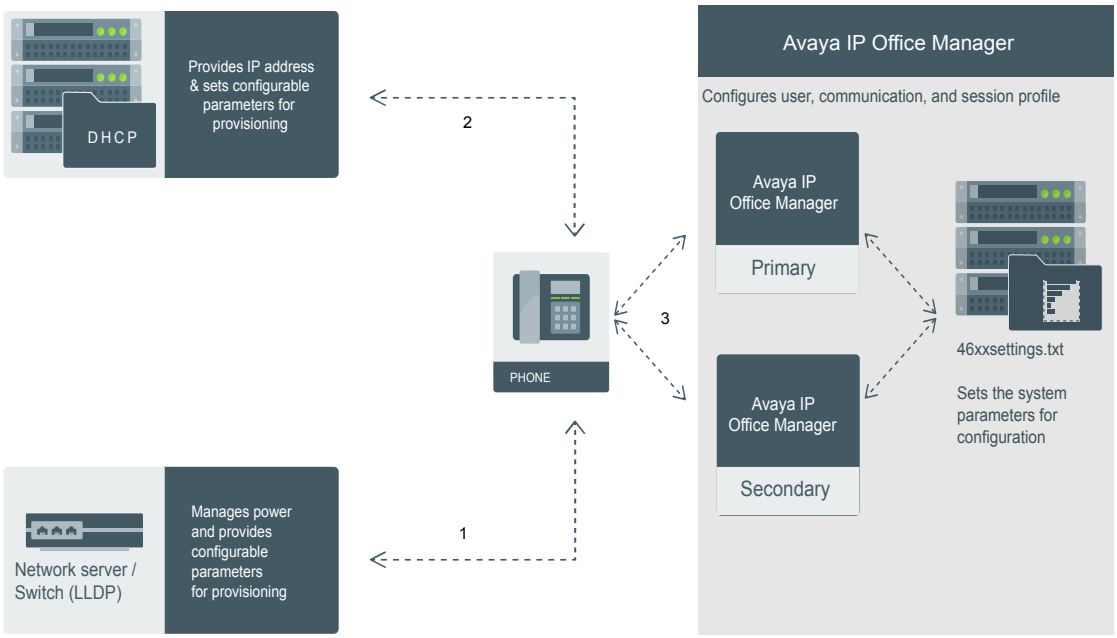


Figure 4: Setup in IP Office environment

DHCP options

You can configure the following options in the DHCP server:

Option	Description
Option 1	Specifies the subnet mask of the network.
Option 3	Specifies the gateway IP address list. The list can contain up to 127 total ASCII characters. Separate more than one IP address with commas with no intervening spaces.
Option 6	Specifies the DNS server address list. The list can contain up to 127 total ASCII characters. Separate more than one IP address with commas with no intervening spaces. The phone supports DNS and the dotted decimal addresses. The phone attempts to resolve a non-ASCII-encoded dotted decimal IP address by checking the contents of DHCP Option 6. At least one address in option 6 must be a valid, nonzero, dotted decimal address, otherwise the DNS address fails.

Table continues…

Option	Description
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.
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. 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

Table continues…

Option	Description
	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.
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

Parameters such as HTTPSRVR and SIP_CONTROLLER_LIST support values with lengths up to 255 octets, but you must set shorter values when you are setting them through DHCP.

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

DHCP site-specific option

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

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

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

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

Parameter	Description
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.

Table continues…

Parameter	Description
	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	Destination port for HTTP requests. The default is 80.
HTTPSRVR	The firmware files are digitally signed, so TLS is not required for security.
ICMPDU	Controls the extent to which ICMP Destination Unreachable messages are sent in response to messages sent to closed ports so as not to reveal information to potential hackers. The default is 1, 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	Controls the Ethernet line interface speed. The default is 1 for auto-negotiate.
PHY2STAT	Controls the secondary Ethernet interface speed. The default is 1 for auto-negotiate.
PROCPSWD	Security string used to access local procedures. The default is 27238.
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.

Note:

In an IP Office environment `J100settings.txt` and `J100Supgrade.txt` files are auto-generated. There is a provision where you can set up a different file server with your own custom Settings file.

DHCP lease time

The DHCP standard states that when a DHCP lease expires, the device should immediately cease using its assigned IP address. However, if the network has problems and the only DHCP server is centralized or if the DHCP server itself has problems, the device will not receive responses to its

request for a renewal of the lease. In this case the device is not usable until the server can respond. Configure system such that once the IP address is assigned to the device, the device continues using that address after the DHCP lease expires, until a conflict with another device is detected.

The system parameter DHCPSTD allows an administrator to specify that the device will either:

- Comply with the DHCP standard by setting DHCPSTD to 1.
- Continue to use its IP address after the DHCP lease expires by setting DHCPSTD to 0.

The latter case is the default. If the default is invoked, after the DHCP lease expires the phone continues to broadcast DHCPREQUEST messages for its current IP address, and it sends an ARP Request for its own IP address every five seconds.

The messages continue to be sent until the device receives a DHCPACK, a DHCPNAK, or an ARP reply. After receiving a DHCPNAK or ARP reply, the device immediately stops using the current IP address. The device displays the DHCPNAK: message for five seconds and then, sets the IP address to 0.0.0.0. Duplicate address detection is no longer performed and the device enters the DHCP INT state.

Depending on the DHCP application you choose, the application might not immediately recycle expired DHCP leases. An expired lease might remain reserved for the original client a day or more. If the client and the DHCP server are in two different time zones, the clocks of the computers are not in sync, or the client is not on the network when the lease expires, there is time to correct the situation.

The following example shows the implication of having a reservation period.

Assume that there are two IP addresses, therefore two possible DHCP leases. Assume that there are three IP devices in the network, two of which are using the two available IP addresses. When the lease for the first two devices expires, the third device cannot get a lease until the reservation period expires. Even if the other two devices are removed from the network, the third device remains without a lease until the reservation period expires.

Parameter configuration through DHCPACK

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

Table continues…

Parameter	Set to
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

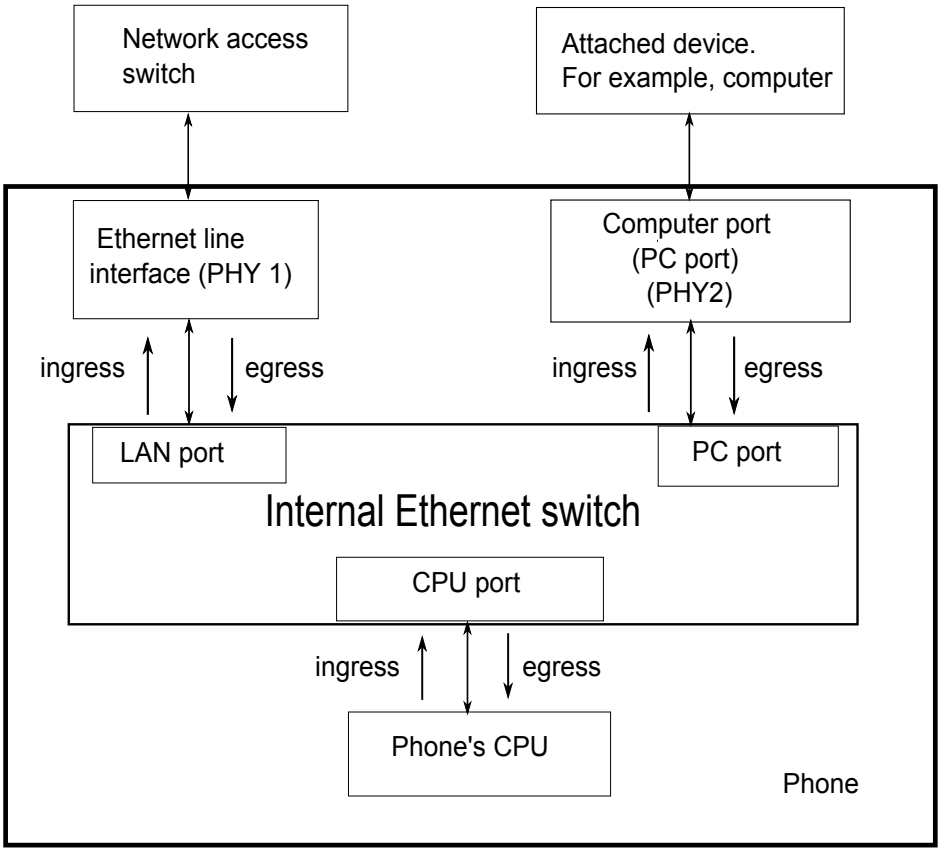
VLANs provide a means to segregate your network into distinct groups or domains. They also provide a means to prioritize the network traffic into each of these distinct domains. For example, a network may have a Voice VLAN and a Data VLAN. Grouping devices that have a set of common requirements can greatly simplify network design, increase scalability, improve security, and improve network management. Therefore, you must always use VLANs in your network.

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 4 byte tag inserted at the beginning of the frame. This additional VLAN tag describes the VLAN ID that a particular device belongs to, and the priority of the VLAN tagged frame. Voice and video traffic typically get a higher priority in the network as they are subject to degradation caused by network jitter and delay.

VLAN separation

The Avaya J129 IP Phone 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 settings 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 settings 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

VLAN separation modes in Avaya J129 IP Phone

Avaya J129 IP Phone 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 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 CPU port and PC port. In order to configure Avaya J129 IP Phone 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.

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.

Exceptions to the VLAN forwarding rules

Exceptions to the VLAN forwarding rules are as follows:

- LLDP frames are always exchanged between the LAN port and CPU port and CPU port and LAN port in all VLAN separation modes.
- 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 LAN and CPU port or PC port, between the PC to CPU port or LAN port and between the CPU port to LAN port in all VLAN separation modes according to DOT1XSTAT and DOT1X configuration.

Special considerations

Special use of VLAN ID of zero

In some configurations it is desirable to utilize the priority functionality of the VLAN frame only and not utilize the VLAN ID properties. In this scenario the phone will add a VLAN tag to the egress voice frames with a VLAN ID = 0 and a priority of the value set by the L2QAUD parameter or L2QSIG parameter.

Automatic failback of VLAN tagging (VLANTEST)

The phone has a functionality that connects the phone 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, it attempts 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 falls back. The phone attempts the DHCP negotiation again in one of the two ways:

- If the VLAN functionality of the phone is turned on (L2Q=1): With a VLANID =0
- If the VLAN functionality of the phone is set to automatic (L2Q=0): Without any VLAN tag.

The parameter that determines how long the phone will wait for a recognizable DHCPOFFER is defined by the VLANTEST parameter. If VLANTEST= 0 then the phone does not failback and keep sending DHCP request using tagged VLAN frames with VLAN ID = L2QVLAN.

Computer port (PC port) VLAN support

The phone only supports one VLAN on the Computer (PC) port, which is the data VLAN, in Full VLAN separation mode. In No VLAN separation mode all VLANs passes between LAN and PC port. However, the CPU port in this case receives all traffic even on VLANs which are not equal to L2QVLAN.

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 a settings file • DHCP option 43 • LLDP
VLANTEST	60	Specifies the number of seconds that the phone waits prior to failing back to a different VLAN ID if no response is received from the DHCP server. Valid values are 0 through 999. Value operation: • 0: The phone continues to attempt a DHCP REQUEST forever. VLANTEST is configured through: • Settings file

Table continues…

Parameter name	Default value	Description
		• A name equal to value pair in DHCPACK message
VLANSEPMODE	1	Specifies whether the VLAN separation is enabled or disabled. Value operation: • 0: Disabled • 1: Enabled VLANSEPMODE is configured through the settings file.
PHY2TAGS	0	Determines whether or not VLAN tags are stripped on Ethernet frames going out of the Computer (PC) port. Value operation: • 0: Strip tags. VLAN tags are stripped from Ethernet frames leaving the computer (PC) port of the phone. • 1: Does not strip tags. VLAN tags are not stripped from Ethernet frames leaving the Computer (PC) port of the phone. PHY2TAGS is configured through the settings file.
L2QVLAN	0	Specifies the voice VLAN ID to be used by IP phones. Valid values are 0 through 4094. L2QVLAN is configured through: • Local admin procedure • A name equal to value pair in DHCPACK message • SET command in a settings file • DHCP option 43 • LLDP
PHY2VLAN	0	Specifies the value of the 802.1Q VLAN ID 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. PHY2VLAN is configured through: • SET command in a settings file • LLDP
L2QAUD	6	Specifies the value of the VLAN priority portion of the VLAN tag when the phone generates tagged Ethernet frames from the internal CPU of the phone. These values are inserted into the VLAN tag for audio frames (RTP, RTCP, SRTP, SRTCP). All other frames except those specified by the L2QSIG parameter are set to priority 0. Valid values are 0 through 7. L2QAUD is configured through: • SET command in a settings file • LLDP
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. L2QSIG is configured through: • SET command in a settings file • LLDP

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, administer VLANs, DSCP and 802.1p priority fields and provide some administration.

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 (01:80:c2:00:00:0e).

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 will not begin until or unless an LLDP frame is received, and the first LLDP frame will be transmitted within 2 seconds after the first LLDP frame is received. Once transmission begins, an LLDPDU will be transmitted every 30 seconds. There could be a delay of up to 30 seconds in phone initialization if the file server address is delivered by LLDP and not by DHCP.

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

LLDPDU transmitted by the phones

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

Table continues…

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

Table continues…

System parameter name	TLV name	Impact
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. 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 TLV = 1, L2Q set to 1 (On). If TLV = 2, L2Q set to 2 (Off).

Table continues…

System parameter name	TLV name	Impact
		If TLV = 3, L2Q 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.

TCP and UDP ports

Avaya J129 IP Phone use different protocols, such as TCP, TLS, and UDP to communicate with other equipment in the network. Part of this communication identifies which TCP or UDP ports each piece of equipment uses to support each protocol and each task within the protocol. Depending on your network, you need to know what ports or ranges are used in the operation of the phones.

Received packets (destination = SIP phone)

Destination port	Source port	Use	Protocol UDP or TCP
The number used in the Source Port field of the packets that the HTTP client of the phone sends	Any	Packets that the HTTP client of the phone receives	TCP
The number used in the Source Port field of the TLS/ SSL packets that the HTTP client of the phone sends	Any	TLS/SSL packets that the HTTP client of the phone receives	TCP
68	Any	Received DHCP messages	UDP
SIP messages initiated by the call server should be sent to the port	Any	Received signaling protocol	TCP

Table continues…

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

Transmitted packets (source = SIP phone)

Destination port	Source port	Use	Protocol UDP or TCP
53	Any unused port number	Transmitted DNS messages	UDP
67	68	Transmitted DHCP messages	UDP
80, unless explicitly specified otherwise	Any unused port number	Packets transmitted by the HTTP client of the phone	TCP
123	Any unused port number	Transmitted SNTP messages	UDP
The number used in the Source Port field of the SNMP query packet received by the phone	161	Transmitted SNMP messages	UDP

Table continues…

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

Chapter 5: Avaya Aura configuration for phones

SIP phone administration on Communication Manager

The SIP-based calling features in the following table can be invoked directly on Avaya J129 IP Phone 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

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 J129 IP Phone 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 J129 IP Phone 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.
- 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 J129 IP Phone 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 to Release 7.1*
  - *Administering Avaya Aura® System Manager for Release 7.1*
  - *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 6: Security

Security overview

SIP-basedAvaya J129 IP Phone 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.

Following security features are available:

- Account management: Supports storage of passwords and user credentials using Federal Information Processing Standards (FIPS 140–2).
  - Supports FIPS 140-2 cryptographic algorithms for application, processes, and users.
  - Supports Identity certificate installation using the following methods:
    - Enrollment using Simple Certificate Enrollment Protocol (SCEP): Requires creating a private key and Certificate Signing Request (CSR) using SCEP interface.
    - Importing key and certificate: Uses an encrypted PKCS#12 file format to import both private key and certificate.
- Certificate management: Supports X509v3 compliant certificates.
  - Supports Public Key Infrastructure (PKI) for users that use third-party certificates for all Avaya services including database.
  - Supports Online Certificate Status Protocol (OCSP) for public key management.
- Supports VLAN separation mode using system parameter.
- Supports synchronization of system clock at configured intervals using system parameter.
- Supports display of SSH fingerprint in the ADMIN menu.
- Displays version of OpenSSH and OpenSSL in the ADMIN menu.
- Under Denial of Service (DoS) attack, the phone maintains integrity and goes to out-of-service mode.
- Supports Open SSL version of random number generator in TLS mode.
- Supports SHA2 hash algorithm and strong encryption (256 bit symmetric and RSA 2048 and 4096 bit asymmetric keys) in TLS mode.
- Supports SRTP/SRTCP and TLS v1.2.

Important:

The ADMIN menu provides access to certain administrative procedures from the phone. You must change the default password for the ADMIN menu to restrict users from using the administrative procedures to change the phone configuration.

Remote access to the phone is completely disabled by default.

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

- SET ENFORCE_SIPS_URI 1
- SET SDPCAPNEG 1
- SET MEDIAENCRYPTION X,9. Recommended values for X are 1 (aescm128-hmac80) or 10 (aescm256-hmac80).

Access control and security

Phones provide several security features for control and access. These are available as:

Security event logging

The logs are maintained for the following events:

- Successful and failed logins, username lockouts, registration and authorization attempts by user and administrators.
- Change in roles.
- Firewall configuration changes.
- Modification or access to the 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 supplicants. EAP-TLS/MD5 password are sent to the WPA supplicants securely.

Temporary Data

The phone deletes any temporary storage data from the program, variables, cache, main memory, registers, and stack.

IP information

The phone enables the user with ADMIN privileges to see the IP information on the phone screen.

The parameter PROVIDE_NETWORKINFO_SCREEN controls the display information.

OpenSSH/OpenSSL version

The phone displays the version of OpenSSL and OpenSSH on the VIEW screen under the ADMIN 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

This feature allows the phone to synchronize the time with the configured NTP servers in intervals. The parameter SNTP_SYNC_INTERVAL checks the time interval for synchronization.

- Default: 1440 minutes
- 60–2880 minutes

Certificate management

Certificates are used to establish secure communications between the network entities. Server or mutual authentication can be used to establish a secure connection between a client and a server. The client always validates the server's certificate. The client 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. If the server does require mutual authentication, the client must have an identity certificate installed to establish secure connection.

The phones support three types of certificates, trusted certificates, On Line Certificate Status Protocol (OCSP) trust certificates, and identity certificates. The Trusted and OCSP trust certificates are root or intermediate Certification Authority (CA) certificates that are downloaded from the server. Identity certificates contain the digital signature with a Public Key that verifies whether the Public Key belongs to the client.

There are enhancements for installing identity certificates:

- SCEP over HTTPS is supported for enrollment.
- PKCS#12 file format support for installation.

For monitoring identity certificate expiry, the parameter CERT_WARNING_DAYS checks the remaining number of days for expiry. 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.

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

Identity certificates

Identity certificates are the endpoint or Server certificates. To share the identity, a public key is presented for identification. X509v3 compliant certificates are supported. Secure communications

that use Transport Layer Security (TLS) or use certificates for authentication purposes are supported to participate in a Public Key Infrastructure (PKI). The following mechanisms are supported for installation:

- Certificate enrollment: Creates a private key and Certificate Signing Request (CSR). CSR is sent to the Certificate Authority (CA) using manual or automatic Simple Certificate Enrollment Protocol (SCEP) interface. Certificate is validated and accepted when CA signs the CSR.
- Importing Key and Certificate: Uses an encrypted PKCS #12 file format to import both the private key and the corresponding certificate.

You can view the following attributes of the certificate using an SNMP MIB browser:

- **Serial Number**
- **Subject Name**
- **Issuer Name**
- **Validity Period**:**notBefore** and **notAfter** dates
- **Thumbprint**: Hash of the certificate
- **Basic Contraints**
- **Subject Alternative Name**
- **Key Usage Extensions**
- **Extended Key Usage**

To validate identity of a received certificate, the following process is followed:

- Verification of certificate chain up to the trusted entity.
- Verification of the signature.
- Verification of the revocation status through OCSP.
- Verification of the certification validity (not-before and not-after dates are checked).
- Verification of the certificate usage restrictions.
- Verification of the identity against the certificate.

Subject Alternative Field (SAN)

SAN field simplify server configuration. With SAN field, you can specify additional host names such as, IP addresses or common names, to use a single SSL Certificate. While validating the certificates, the phone verifies whether the presented certificate has a SAN field or not.

- If the certificate does not have the SAN field, the phone validates the Common Name (CN) fields of the certificate. In this case, you need the following CN fields:
  - **SIP domain name**
  - **IP address**
- If the SAN field is present in the certificate, following are the attributes specific to the connection type:

  For SIP-TLS connection

  - With valid SIP URIs
    - SIP URI attribute should have SIP domain name as value.

- IP attribute must have the IP address of LAN as value.

- Without valid SIP URIs
  - DNS attribute with SIP domain as value.
  - IP attribute with IP address of LAN as value.

For HTTP-TLS connection

- Provisioning phone with only IP address
  - In the **SAN** field, IP attribute with IP of HTTPS server as value.
- Provisioning phone with FQDN of HTTPS server
  - In the **SAN** field, IP attribute with the IP address of HTTPS server as value.
  - DNS attribute with FQDN of HTTPS server as value.

Note:

While provisioning the phone with FQDN of HTTPS server, you need two attributes in the **SAN** field:

- DNS attribute with FQDN
- IP attribute IP address

Trusted certificates

Trusted certificates are the root certificates that are used to verify the received certificates. These are required for establishing TLS sessions and trust domains for deployment. Avaya Aura® System Managerhas a trust management system that verifies the certificates. The trust management system has a Certification authority (EJBCA) who signs the certificate.

The trust management system performs the following operations:

- Lifecycle management of identity certificates for elements.
- Secure storage of Private Keys.
- Issuance of Certificates.
- Revocation of Issued Certificates.
- Publish revocation information for issued certificates.
- Add, view, and delete trusted certificates to create trust domains.

OCSP trust certificates

On Line Certificate Status Protocol (OCSP) trust certificates are installed when the trusted certificates are already installed. OCSP trust certificates are also root (or intermediate) certificates that are downloaded from the file server. OCSP is a protocol that is used for obtaining the revocation status of an X.509 digital certificate. A new trust store is created to store OCSP trust certificates on the phone.

Parameter 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 7: 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: The default password is `27238`. You must not 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**.

Accessing the Admin menu after log in

Procedure

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

Accessing the IPv4 settings

Procedure

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

4. Select **IP Configuration** > **IPv4**.

   The phone displays the parameters for IP configuration.

IP configuration field description

Configuration Parameter Name	Description
The following parameters are available in 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`.
Router	Specifies the router IP address. 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. • **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.

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 settings file parameter that is capable of receiving a phone report from the phone.

Procedure

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

   The phone displays the following debug options:

   - **Phone Report**
   - **Port Mirroring**
   - **SSH**
   - **SSH fingerprint**
   - **Svc control**
   - **Svc record**

   Note:

   The options in the debug mode can be modified if an authentication file is installed.
5. Use the appropriate keys to enable or disable the options.
6. Press **Save**.
7. Restart the phone.

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. Select **Ethernet interface**.

5. Use the **Down Arrow** key to select one of the following settings:
   - **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**.

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** > **Admin**.
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**.

Setting event logging

Procedure

1. Press **Main Menu** > **Admin**.
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**.

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 auto generated J100 settings file 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** > **Admin**.
2. In the **Access code** field, enter the admin 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** > **Admin**.
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.	
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

Table continues…

Setting	Description	Associated Configuration Parameter
DNS Server	The IP address of the DNS server that the phone accessed before successfully.	DNSSRVR_IN_USE
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** > **Admin**.
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 admin menu.

Chapter 8: 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** > **Admin**.
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 system values and system initialization values except AUTH and AUTH_ONLY to default values.
   - The 802.1X ID and Password to their default values.
   - Call server values to their defaults.
   - Any entries in the Redial buffer.
   - Does not affect user-specified data and settings like Contacts data or the phone login and password.

   Note:

   Avaya J129 IP Phone parameters stored for a particular user are not reflected in other phones, for example, 9600 Series IP Deskphones, even if the SIP user is the same.

Device upgrade overview

Before upgrading the device, ensure that you download the latest software, the distribution package and the settings file, on the file server. You can perform the device upgrade in the following way:

- Manual: You can upgrade the device without the device waiting for a polling interval by:
  - Using the update option in the Settings app on the device. With the update option, the device immediately downloads and installs the software if an updated version is available.
  - Rebooting the device from the Settings app or from System Manager. With rebooting, the device might upgrade immediately or later based on the upgrade policy configured for the device.

Device upgrade process

The upgrade event is logged under NOTICES level in the Syslog file. During boot up, the Avaya J129 IP Phone performs the following tasks:

1. The phone receives the file server address from DHCP, LLDP, or the device interface.
2. The phone connects to the file server and searches for the upgrade file.

   Note:

   In IP Office, the upgrade file is auto generated.
3. The phone compares its software version with the version specified in the upgrade file.
4. The phone then downloads the upgrade file for parsing. The parameter CONFIG_FILE_EXECUTION_STATUS is updated with the following values upon parsing:
   - 0: Upgrade file is downloaded and parsed.
   - 1: Upgrade file is downloaded but not parsed.
   - 2: Upgrade file is not downloaded and not parsed.
5. The upgrade gets triggered depending on the parameter CONFIG_FILE_EXECUTION_STATUS value.
6. The phone starts downloading files depending on the firmware filename defined by APPNAME value contained in the upgrade file.
7. The phone downloads the software files and upgrades itself if no fatal error occurs.

   Tip:

   Fatal error occurs when:
   - The file size is large.
   - The signature is missing.

- The signature validation fails.
- The file is not found.
- The file fails to download.
- The file is not compatible with the hardware.
- The file fails to write to the flash memory.
- There is any parsing error.

Manual upgrade

About this task

Use the Avaya-provided upgrade script files and the application files that are included in the zip files to upgrade the phones. Ensure that all the files are together on the file server. Do not modify the files. Use this procedure to download the latest version of the software to the file server.

IP Office auto generates `J100Supgrade.txt` and `J100settings.txt` files. These files must be used in IP Office environment.

Procedure

1. Stop the file server.
2. Specify the port settings for HTTP or TLS in the HTTPPORT or TLSPORT settings respectively.
3. Perform a back up of all the current file server directories.
4. Copy the `46xxsettings.txt file` to a backup location.
5. Remove all the files in the download directory. This ensures that you do not have an inappropriate binary or configuration file on the server.
6. Download the self-extracting executable file or the corresponding zip file.
7. Extract all the files.
8. Copy the `46xxsettings.txt file` to the download directory.
9. Check the `Readme` file for release-specific information.
10. Modify the `46xxsettings.txt file` as required.
11. Restart the HTTP/HTTPS server.
12. Reset the phone.

Related links

Downloading and saving the software on page 21

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 to enable the lock screen password.
SHOW_CALL_APPEARANCE_NUMBERS	0	Specifies whether for a user the device displays call appearance numbers in the call containers.

Chapter 9: System failover

Supported SIP environments

Avaya J129 IP Phone work on the following environments:

- Avaya Aura® Session Manager with Avaya Aura® Communication Manager
- IP Office
- Failover and survivable interoperability with the following SIP gateways:
  - Session Manager for survivable remote gateway
  - Avaya Secure Router 2330 and 4134
  - Audiocodes MP-series analog and BRI gateways
  - Avaya Aura® Media Server 7.7.0.334.
  - IP Office

For information about configuring the phone features, see the following documents:

- *Avaya Aura® Communication Manager Feature Description and Implementation*
- *Administering Avaya Aura® Communication Manager*
- *Avaya IP Office™ Platform SIP Telephone Installation Notes*

Failover and survivability overview

The phone detects a network or server failure in approximately 90 seconds. After a failure is detected, the phone selects an active controller in approximately five seconds. During network or server failures, multiple controllers or servers are supported for the following operations:

- Making a call including emergency calls
- Receiving a call
- Call transfer
- Call forward
- Mid call features: Call hold and mute
- Audio Conference: Local three-way audio conference

Phone resiliency and transition states

The transition states happens in the following order:

- Limbo: Connection to the primary server is lost but the failover is not detected.
- Moving Subscriptions Interval (MSI): Connection to the primary server is lost, and the phone is currently registered to the survivability server. Successful subscription to the survivability server is incomplete.
- Acquiring services: Connection to the primary server is lost, and the phone displays the following message in the idle state:

  ```
  Acquiring Service
  ```

- Failover to the secondary/survivability server: Connection to the secondary/survivability server is active. All the supported features are also active. The phone performs the following intermediate steps:
  - Selection of active controller: The phone attempts to select the monitored active controller.
  - Successful subscription: Connection to the monitored controller is made with successful subscription.
  - Call/media preservation: During an active call, the phone detects that the connection is lost with the primary controller and the call/media is preserved. Media preservation is only available in an Avaya Aura® environment.
  - Advanced SIP Telephony (AST) feature determination: The phone verifies whether the controller supports the AST feature. AST feature is only available in an Avaya Aura® environment.
  - Personal Profile Manager (PPM) synchronization: When AST mode is determined and enabled, then the phone starts the PPM synchronization process. PPM is only available in an Avaya Aura® environment.
- Failback to the primary server: Connection to the primary server is established when the phone detects that the primary server is functional again. The changes that were cached earlier are now synced with the PPM server. Failback doesn’t happen during an active call.

Avaya J129 IP Phone survivability in the Avaya Aura® environment

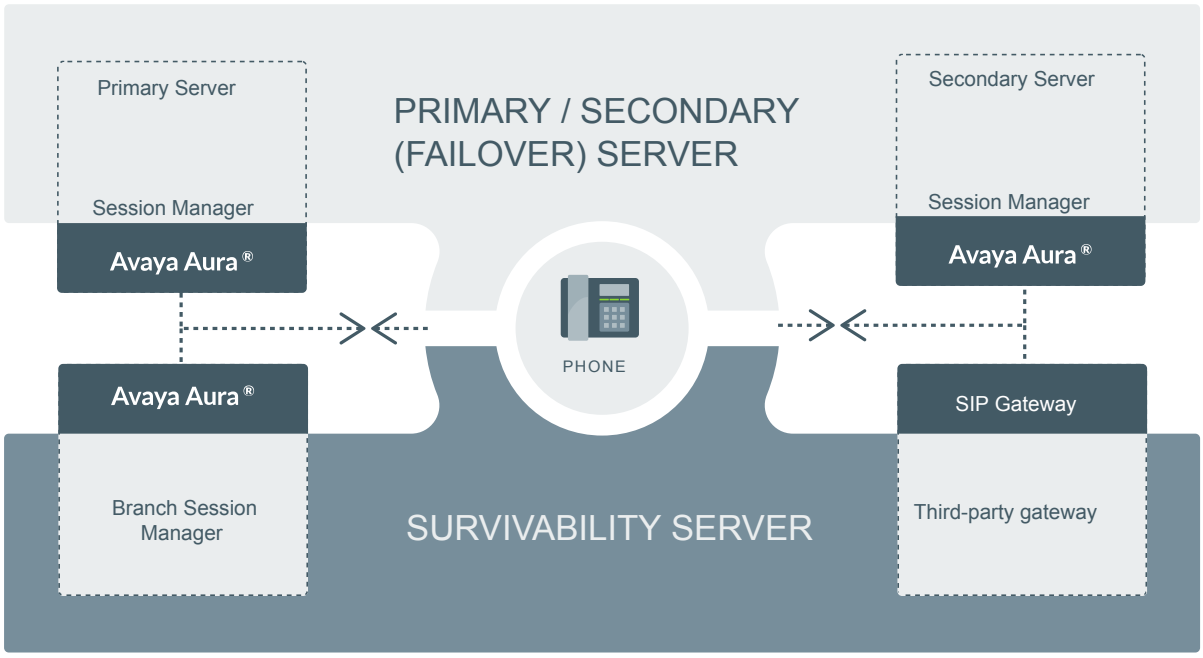


Figure 5: Survivability in Avaya Aura®

Note:

For more information on survivability about IP Office environment, see *Administering Avaya IP Office Platform with Web Manager*.

Survivability controller determination

The order of precedence in determining the active controller is:

1. Phone user interface
2. PPM server
3. Settings file

4. DHCP server (Option 242)

The phone performs the DNS queries to resolve hostnames and the signaling protocol. The order is set as TLS, TCP, and then UDP when there is no DNS NAPTR or SIP URI. The phone sends the SIP REGISTER request for each CONTROLLER_SEARCH_INTERVAL. The phone retries the monitoring attempt using the RECOVERYREGISTERWAIT parameter.

If the value of the SIPREGPROXYPOLICY parameter is alternate and a user is logged in, the phone maintains a single active SIP registration. SIP registration is done with the highest priority available controller. Also, the parameter FAILBACK_POLICY controls the SIP registration priority. If the FAILBACK_POLICY parameter is configured with automatic instead of admin, then the phone's active controller has the highest priority.

If the value of the SIPREGPROXYPOLICY parameter is simultaneous and a user is logged in, the phone maintains all active SIP registrations. The phone simultaneously registers using the value provided in the SIMULTANEOUS_REGISTRATIONS and SIPDOMAIN parameters.

The phone uses a SIP URI instead of SIPS URI unless SRTP is enabled. When registration is successful, the phone sets the SIPPROXYSRVR_IN_USE parameter to the IP address of this active controller.

The phone starts a search for a new active controller whenever it encounters one of the following triggers :

- Trigger 1: The TCP socket closes or TCP Keep-alive timeout occurs.
- Trigger 2: The phone receives an administrative failback trigger from a Configured Controller.
- Trigger 3: Fast Response Timer.
- Trigger 4: The phones receives n incoming INVITE from a non-active controller.
- Trigger 5: Re-registration with the active controller is timed out.

Advanced SIP Telephony feature determination

The parameter DISCOVER_AVAYA_ENVIRONMENT determines whether the selected controller supports the Advanced SIP Telephony (AST) feature. When the parameter value is set to 1, the phone sends a SUBSCRIBE request to the active controller for the Feature Status Event Package (avaya-cm-feature-status).

The phone determines the AST mode based on the response 202. Then it starts an internal timer of 16 seconds and waits to receive a NOTIFY message as `active`.

If the phone does not receive a NOTIFY message and receives a termination message instead, then the non-AST mode is enabled. Synchronization with the Personal Profile Manager (PPM) server starts when the AST mode is enabled.

Synchronization with the Personal Profile Manager server

The phone performs the synchronization with the Personal Profile Manager (PPM) server only when the `getAllEndpointConfiguration` request is successful. If the

`getAllEndpointConfiguration` request is unsuccessful, the `getContactList` request is also ignored. This request contains the following fields:

- VolumeSettings
- LinePreferenceInfo
- ListOfOneTouchDialData
- ListOfButtonAssignments
- SoftMenuKeyList
- DialPlanData
- ListOfSpeedDialData
- ListOfMaintenanceData
- ListOfTimers
- VMONInfo
- ListOfRingerOnOffData
- ListOfNumberFormatRules: Applicable only when registered to Avaya Aura® Session Manager.
- ListOfIdentities: Applicable only when registered to Avaya Aura® Session Manager.

  MWExt: Applicable only when registered to Avaya Aura® Session Manager.
- VMNumber: Applicable only when registered to Avaya Aura® Session Manager.

Provisioning survivability for SIP phones

About this task

Use this procedure to provision survivability.

In IP Office environment, survivability is provisioned in the auto generated Settings file..

Procedure

1. Set the applicable failover configuration parameters in the `46xxsettings.txt file` file.
2. Provision the gateway per the Application Notes, available on the Avaya support Web site.
3. Load the latest SIP Release software and associated files on the file server.
4. Reboot all registered phones from SIP Enablement Services or Avaya Aura® Session Manager.
5. Power up other phones.

Configuring survivability

Use the `46xxsettings file` to set these parameters.

In IP Office, the auto generated `J100 settings file` has the all the details of these parameters.

By administering survivability configuration parameters using the `46xxsettings file` (or using the default values if applicable), the SIP phones can quickly switch to an active controlling server and experience minimal disruption. The failover/failback parameters are:

- CONTROLLER_SEARCH_INTERVAL - The time the phone waits to complete the maintenance check for Monitored Controllers.
- DISCOVER_AVAYA_ENVIRONMENT - Determines whether the phone operates in a mode to comply with the Avaya environment mode (provision of SIP/AST features and use of PPM for download and backup/restore).
- ENABLE_REMOVE_PSTN_ACCESS_PREFIX - Enables the removal of the PSTN access prefix from collected dial strings when the phone is communicating with a non-AST controller.
- FAILBACK_POLICY - Failback Policy.
- FAST_RESPONSE_TIMEOUT - Fast Response Timer.
- PSTN_VM_NUM - The number called when the phone is in failover and the Message button is pressed.
- RECOVERY_REGISTER_WAIT - Reactive Monitoring Interval in seconds.
- REGISTERWAIT - Proactive Monitoring Interval in seconds.
- SIP_CONTROLLER_LIST - Configured Controller list. A comma-separated list of SIP URIs, a hostname, or numeric IP address. If null, DHCP/DNS will provide the defaults.
- SIMULTANEOUS_REGISTRATIONS - The number of Session Managers with which the phone will simultaneously register.
- SIPREGPROXYPOLICY - Registration Policy. The default value of this parameter is `simultaneous`.

Configuring AudioCodes server for survivability

If you set AudioCodes server in the Avaya environment for survivability, you must configure the following options:

- Connection reuse
- Connection reuse in survivability mode
- Record-Route

Enabling connection reuse

Procedure

1. Go to the audio codes URL and click **Configuration** > **VoIP** > **SIP Definitions** > **General Parameters**.
2. Set **Enable TCP Connection Reuse** to *Enable*.
3. Click **Submit**.

Enabling connection reuse in a failover environment

Procedure

1. Go to the audio codes URL and click **Configuration** > **VoIP** > **SAS** > **Stand Alone Survivability**.
2. Set **SAS Connection Reuse** to *Enable*.
3. Click **Submit**.

Enabling Record Route in invite messages

Procedure

1. Go to the audio codes URL and click **Configuration** > **VoIP** > **SAS** > **Stand Alone Survivability**.
2. Set **Enable Record-Route** to *Enable*.
3. Click **Submit**.

User experience during failover

Feature	Normal Operation with Communication Manager	Failover Operation with a Generic SIP Gateway	IP Office branch mode
Make call	Yes	Yes	Yes
Receive call	Yes	Yes	Yes
Call Hold	Yes	Yes	Yes
Consultative Hold	Yes	Yes	Yes
Ad hoc conferencing	Yes, up to 6 parties	Yes, up to 3 parties	Yes, up to 3 parties

Table continues…

Feature	Normal Operation with Communication Manager	Failover Operation with a Generic SIP Gateway	IP Office branch mode
Forward all my calls/SAC	Yes	Yes	Yes In IP Office the feature is handled using shortcodes.
Forward my calls when busy/no answer	Yes	Yes	Yes In IP Office the feature is handled using shortcodes.
Attended call transfer	Yes	Yes	Yes
Inbound call management	Yes (Communication Manager COR)	Yes (depends on local proxy capabilities and provisioning)	Yes (depends on local proxy capabilities and provisioning)
Outbound call management	Yes (Communication Manager COR)	Yes (proxy)	Yes (proxy)
Calling party block	Yes	No	No
Call park	Yes	No	Yes In IP Office the feature is handled using shortcodes.
Call unpark	Yes	No	Yes In IP Office the feature is handled using shortcodes.
Auto callback	Yes	No	No
Malicious call trace	Yes	No	No
EC500 on/off	Yes	No	No
Transfer to voice mail	Yes	No	No
Extend-call	Yes	No	No
Hold recall	Yes	No	No
Transfer recall	Yes	No	No
Message waiting indicator	Yes	No	No

Note:

If the phone displays the message `Limited phone service`, press **OK** to acknowledge and clear the message.

Chapter 10: 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, ensure the following:
   - SIP proxy servers must be specified by IP address and not by FQDN.
   - There must only be two proxy servers configured.

   The circle is filled in if the connection is properly configured. Circle with a line through it is 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 11: Related 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 for Release 7.1	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

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. Click **Enter**.

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 http://support.avaya.com and perform one of the following actions:
  - 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 perform one of the following actions:
  - 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 http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Appendix A: List of configuration parameters

Parameter name	Default value	Description
A		
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 (default).
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 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 **Admin** menu. Valid values are from 5 min. to 1440 min.
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.
AUDIOSTHS		Specifies the level of sidetone in the handset.
AUTH		Specifies whether the script files are downloaded from an authenticated server over an HTTPS link. Value Operation • 0: Optional • 1: Mandatory

Table continues…

Parameter name	Default value	Description
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 (default). • 1: Enhanced debugging capabilities are enabled. The parameter must be set to 1 only for the debugging period by Avaya technicians. Set the parameter back to 0 when the debugging period completes.
B		
BRANDING_VOLUME	5	Specifies the volume level at which the Avaya audio brand is played. Value Operation • 8: 9db above nominal • 7: 6db above nominal • 6: 3db above nominal • 5: nominal (default) • 4: 3db below nominal • 3: 6db below nominal • 2: 9db below nominal • 1:12db below nominal
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, the administrator must access the Admin menu of the phone and select **Phone report**.
C		
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.

Table continues…

Parameter name	Default value	Description
CALLFWDSTAT The parameter is only available in an Avaya Aura® environment.	0	Sets the call forwarding mode of the phone by summing following the 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 remaining for certificate expiry. Valid values are from 0 to 99.
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.
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. If the parameter is set to a value that is outside the range then default value is selected.

Table continues…

Parameter name	Default value	Description
		Note: The parameter is set to 0 in IP Office environment.
CONFIG_SERVER_SECURE_MODE	1	Specifies whether HTTP or HTTPS is used to access the configuration server. Value Operation • 0: HTTP • 1: HTTPS • 2: Use HTTPS if SIP transport mode is TLS, otherwise use HTTP. This parameter is not supported in IP Office environment as PPM is not supported.
CONNECTION_REUSE	1	Specifies whether the phone will use two UDP, TCP, or TLS connection (for both outbound and inbound) or one UDP, TCP, or TLS connection. Value Operation • 0: Disabled. The phone opens oubound connection to the SIP Proxy and listening socket for inbound connection from SIP proxy in parallel. • 1: Enabled. The phone does not open a listening socket and will maintain and re-use the sockets it creates with the outbound proxies. **Note:** On Avaya J129 IP Phone, only 1 is 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		Specifies the number of seconds the phone will wait to complete the 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.

Table continues…

Parameter name	Default value	Description
		• 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.
CURRENT_CONTENT	Null	Specifies the URL of an XML file that is used to customize the home screen.
CURRENT_SKIN		Specifies the skin for display layout When you set the parameter (not empty string), then that particular skin is selected for display. This parameter must be one of the label as defined in SKINS configuration parameter. If the parameter is empty or not set, then default skin is used.
D		
DATEFORMAT		Specifies the format for dates displayed in the phone. • Use %d for day of month • Use %m for month in decimal format. • Use %y for year without century (e.g., 07). • Use %Y for year with century (e.g., 2007). Any character not preceded by % is reproduced exactly.
DELETE_MY_CERT	0	Specifies to remove the installed identity certificates without CLEAR operation. Value operation: • 0: (Default) Disabled. • 1: Enabled.

Table continues…

Parameter name	Default value	Description
DHCPSTD	0	Specifies if DHCP complies with the IETF RFC 2131 standard: • And immediately stops using an IP address if the lease expires • Or if it will enter an extended rebinding state in which it continues to use the address and to periodically send a rebinding request • To periodically send an ARP request to check for address conflicts, until a response is received from a DHCP server or until a conflict is detected. Value Operation • 0: Continue using the address in an extended rebinding state. • 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 **Admin** 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.
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. • 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.

Table continues…

Parameter name	Default value	Description
DSCPSIG	34	Specifies the layer 3 Differentiated Services (DiffServ) Code Point for signaling frames generated by the phone. 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		
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 SES with AST features and PPM. **Note:** Set the parameter to 0 for IP Office environment.
ENABLE_CALL_LOG		Species if call logging and associated menus are available on the phone.

Table continues…

Parameter name	Default value	Description
		Value Operation • 0: No • 1: Yes
ENABLE_CONTACTS	1	Specifies if the contacts application and associated menus are available on the phone. Value Operation • 0: No • 1: Yes **Note:** The parameter is set to 0 for IP Office environment.
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 • 1: Yes Setting this parameter to 1 can speed up call setup.
ENABLE_G711A	1	Specifies if the G.711 a-law codec is enabled. Value Operation • 0: Disabled • 1: Enabled
ENABLE_G711U	1	Specifies ifr the G.711 mu-law codec is enabled. Value Operation • 0: Disabled • 1: Enabled
ENABLE_G722	1	Specifies if the G.722 codec is enabled. Value Operation • 0: Disabled • 1: Enabled
ENABLE_G726	1	Specifies if the G.726 codec is enabled. Value Operation • 0: Disabled • 1: Enabled

Table continues…

Parameter name	Default value	Description
ENABLE_G729	1	Specifies if the G.729A codec is enabled. Value Operation • 0: Disabled • 1: Enabled without Annex B support (default). • 2: Enabled with Annex B support.
ENABLE_HOLD_BUTTON	1	Specifies whether a **Hold** softkey will be displayed during an active call. Value Operation • 0: Hold softkey is not displayed. • 1: Hold softkey is displayed (default).
ENABLE_IPOFFICE	0	Specifies whether the deployment environment is IP Office Value Operation • 0: Not an IP Office environment. • 1: IP Office environment. **Note:** Set DISCOVER_AVAYA_ENVIRONMENT parameter to 0 when the phone is set up in IP Office environment
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. 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.

Table continues…

Parameter name	Default value	Description
		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	1	Specifies if on the idle phone screen, a softkey and a feature button must be displayed to allow users to manually lock the phone. Value Operation • 0: Disabled. **Lock** softkey and feature button is not displayed. • 1: Enabled. **Lock** softkey and feature button is displayed.
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_PRESENCE		Specifies if presence will be supported. Value Operation • 0: Disabled

Table continues…

Parameter name	Default value	Description
		• 1: Enabled **Note:** This parameter is set to 0 in IP Office environment.
ENABLE_REDIAL		Specifies if **Redial** softkey is available. Value Operation • 0: No • 1: Yes
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. 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 if **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 if 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.

Table continues…

Parameter name	Default value	Description
		• 2: **Emergency** softkey is displayed with a confirmation screen. **Note:** The parameter is set to 0 for IP Office environment.
ENCRYPT_SRTCP	0	Specifies whether RTCP packets are encrypted or not. 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. Value Operation • 0: Disables algorithm. • 1: Enables algorithm, but not for contacts. **Note:** The parameter is set to 0 for IP Office environment.
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. Valid values are 0 through 1000. This parameter is used only for development and debugging purposes.
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.

Table continues…

Parameter name	Default value	Description
		Valid values are 5 through 999. The default value is 30.
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 the usage of FIPS-140 approved cryptography is enabled or not. Value Operation • 0: (Default). Disables FIPS-140 approved cryptographic algorithms. • 1: Enables only FIPS-140 approved cryptographic algorithms.
FQDN_IP_MAP	Null	Specifies to validate an FQDN contained in the certificate when IP address is used to establish the connection. The parameter is a comma separated list of name or value pairs where the name is an FQDN and the value is an IP address.
G		
G726_PAYLOAD_TYPE	110	Specifies the RTP payload type to be used for the G.726 codec. Valid values are 96 through 127.
GMTOFFSET	0:00	Specifies the time offset from GMT in hours and minutes. The format begins with an optional + or - (+ is assumed if omitted), followed by 0 through 12 (hours), followed by a colon (:), followed by 00 through 59 (minutes).
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.
H		
HANDSET_PROFILE_DEFAULT	1	Specifies the number of the default handset audio profile.

Table continues…

Parameter name	Default value	Description
		Valid values are 1 through 20.
HANDSET_PROFILE_NAMES	NULL	Specifies an ordered list of names to be displayed for handset audio profile selection. The list can contain 0 to 255 UTF-8 characters. Names are separated by commas without any intervening spaces. Two commas in succession indicate a null name, which means that the default name should be displayed for the corresponding profile. Names might contain spaces, but if any do, the entire list must be quoted. There is no way to prevent a profile from being displayed.
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.
I		
INGRESS_DTMF_VOL_LEVEL	-12dBm	Specifies the power level of tone, expressed in dBm0. Values can range from -20dBm to -7dBm.
INTER_DIGIT_TIMEOUT	5	Specifies the number of seconds that the phone waits after a digit is dialed before sending a SIP INVITE. Valid values are 1 through 10.
K		
L		
L2Q	0	Specifies whether the VLAN tagging is enabled or disabled.

Table continues…

Parameter name	Default value	Description
		Value Operation • 0: Auto - VLAN tagging is turned on when the network can support VLAN tagging and L2QVLAN is non zero. • 1: On - VLAN tagging is turned on when the network can support VLAN tagging. The IP phone sends tagged frames with VLAN = L2QVLAN, even if L2QVLAN is set to 0. • 2: Off - VLAN functionality is disabled. **Note:** This parameter can also be set through: • Local admin procedure • A name equal to value pair in DHCPACK message • SET command in a settings file • DHCP option 43 • LLDP
L2QAUD	6	Specifies the 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.

Table continues…

Parameter name	Default value	Description
		Note: This parameter can also be set through: • SET command in a settings file • LLDP
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
LANGLARGEFONT	Null	Specifies the name of the language file for the display of large text. The file name can contain 0-32 ASCII characters. When you set the parameter to the default value null, the **Text Size** option is not available.
LANGUAGES		Specifies the language files that must 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.
LOCAL_CALL_PREFIX	DIAL_AS_IS	Sets the prefix for local calls. Permissible values are the Area Code denoted by AC, a string of digits, or the default, DIAL_AS_IS.
LOCAL_DIAL_AREA_CODE		Specifies if user must dial area code for calls within same area code regions. Value Operations • 0: User don't need to dial area code. • 1: User need to dial area code. When enabled, the area code parameter (PHNLAC) should also be configured.

Table continues…

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

Table continues…

Parameter name	Default value	Description
		This parameter must be specified to log events below the Error level. The list can contain up to 255 characters. Category names are separated by commas without any intervening spaces. H1xx SIP R1.0 and later; the default is ALL which implies all categories. New categories for H1xx compare to 96x1 SIP include ANDROID and KERNEL.
LOG_DIALED_DIGITS	1	Specifies if the call log will contain digits dialed by a user or information about a remote party when the user dials a FAC code. The FAC code is identified by * or # entered as a first character. Value Operation • 0: Allow dialed FAC code to be replaced with a remote party number in the call history • 1: Dialed digits are logged in call history exactly as they were entered by the user (default).
LOGSRVR	Null	Specifies one address for a syslog server in dotted-decimal formatl (IPv4), colon-hex format (IPv6, if supported), or DNS name format. 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.
MEDIAENCRYPTION	9	Specifies which media encryption (SRTP) options is supported.

Table continues…

Parameter name	Default value	Description
		Up to 2 or 3 options can be specified in a comma-separated list. You can specify 3 options, but only the first two supported options are used. 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 (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 Managerhas the capability to change the list order in the SDP-OFFER (for audio only) when the SDP-OFFER is pass through.
MTU_SIZE		Specifies the maximum transmission unit (MTU) size transmitted by the phone. Valid values are 1496 or 1500. Use 1496 for older Ethernet switches.
MUTE_ON_REMOTE_OFF_HOOK	1	Controls the speakerphone muting for a remote-initiated (a shared control or OOD-REFER) speakerphone off-hook. Value Operation 0: the speakerphone is unmuted 1: the speakerphone is muted

Table continues…

Parameter name	Default value	Description
		The value is applied to the phone only when the phone is deployed with a Avaya Aura® Communication Manager 6.2.2 and earlier releases. If the phone is deployed with Avaya Aura® Communication Manager 6.3 or later, the setting is ignored. Instead the feature is delivered through PPM. The Turn on mute for remote off-hook attempt parameter is enabled in the station form through the Avaya Aura® Session Manager(System Manager) or Avaya Aura® Communication Manager(SAT) administrative interfaces. **Note:** This parameter is set to 0 in IP Office environment.
MWISRVR	Null	Specifies a list of addresses of Message Waiting Indicator servers. Addresses can be in dotted-decimal or DNS name format, separated by commas without any intervening spaces. The value can contain 0 to 255 characters.
MYCERTCAID The parameter is only available in an Avaya Aura® environment.	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.
MYCERTCN	$SERIALNO	Specifies the Common Name (CN) used in the SUBJECT of an SCEP certificate request. The value must be a string that contains either $SERIALNO" (which will be replaced by the phone's serial number) or $MACADDR (which will be replaced by the phone's MAC address), but it can contain other characters as well, including spaces. The value can contain eight ($MACADDR) to 255 characters.
MYCERTDN	Null	Specifies the part the SUBJECT of an SCEP certificate request that is common for all phones. The value must begin with a / and can include Organizational Unit, Organization, Location, State and Country. The value can contain Zero to 255 ASCII characters.

Table continues…

Parameter name	Default value	Description
		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 minimum value is 2048.
MYCERTRENEW	90	Specifies the percentage of the identity certificate's validity interval after which renewal procedure is initiated. Valid values are 1 through 99.
MYCERTURL	Null	Specifies the URL of the SCEP server for obtaining an identity certificate. If the URL is specified in HTTPS, then the HTTPS is used to send the CSR to the SCEP server. The valid values can range from Zero to 255 ASCII characters. The default value is null .
MYCERTWAIT	1	Specifies the phone's behavior if the SCEP server indicates that the 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 that whether the server certificate can be accepted if the result of the revocation check cannot be determined due to missing revocation information • 0: Certificate is considered to be revoked if the certificate revocation status is unknown. TLS connection will be closed.

Table continues…

Parameter name	Default value	Description
		• 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. Valid range is from 60 to 10080
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 • 1: SHA256
OCSP_NONCE	1	Specifies that whether a nonce is added in the OCSP requests and expected in the OCSP responses. Value operation: • 0: Not added. • 1: Added.
OCSP_TRUSTCERTS		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 single locally configured URI of an OCSP responder. Only one URI is permitted and it can obtain an IP address or FQDN. Embedded spaces are not allowed. Valid range if from 0 to 255 ASCII characters.
OCSP_USE_CACHE	1	Specifies that the OCSP caching is in use. Value operation: • 0: Checks the OCSP responder and disables the use of OCSP caching. • 1: Enables the use of OCSP caching.

Table continues…

Parameter name	Default value	Description
OCSP_URI_PREF	1	Specifies the preferred URI for use in an OCSP request when more than one source is available. Value operation: • 1: Checks the OCSP_URI and then the OCSP field of the Authority Information Access (AIA) extension of the certificate. • 2: Checks the OCSP field of the Authority Information Access (AIA) extension of the certificate and then the OCSP_URI.
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).
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.
P		
PER_MODEL_SETTINGS		
PHNCC	1	Specifies the country code for United States. The value is 1. Valid values 1 to 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 3-13.
PHNEMERGNUM	Null	Specifies an emergency phone number to be dialed if the associated button is selected. Valid values can contain up to 30 dialable characters (0-9, *, #).
PHNMOREEMERGNUMS	Null	Specifies list of emergency numbers separated by comma. Valid values may contain up to 30 dialable characters (0-9, *, #).
PHNIC	011	Specifies the international access code

Table continues…

Parameter name	Default value	Description
		For the United States, the value is 011. Valid values are 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 5-15.
PHNMUTEALERT_BLOCK	1	Specifies if the **Mute Alert** feature is blocked or unblocked. Value Operation • 0: Unblocked • 1: Blocked
PHNNUMOFSA	3	Specifies the number of session appearances the phone must support while operating in an non-Avaya environment. Valid values are 1 through 10.
PHNOL	9	Specifies the outside line access code. This is the number you press to make an outside call. Valid values are 0 to 2 dialable characters (0-9, *, #).
PHONE_LOCK_IDLETIME	5	Specifies the interval of idle time, in minutes, after which the phone will automatically lock. The phone will lock only if the value of ENABLE_PHONE_LOCK is 1. If set to 0 the phone will not lock automatically.
PHY1STAT	1	Specifies the speed and duplex settings for the Ethernet line interface.

Table continues…

Parameter name	Default value	Description
		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.
PHY2PRIO	0	Specifies the layer 2 priority value to be used for frames received on the secondary Ethernet interface when VLAN separation is enabled. Valid values are 0 through 7.
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.

Table continues…

Parameter name	Default value	Description
		• 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 coming out of the internal CPU of the phone. Valid values are 0 through 4094. **Note:** This parameter is configured through: • SET command in a settings file • LLDP
PKCS12URL	Null	Specifies the IPv4 or IPv6 URL address or FQDN from where a PKCS#12 file is to be downloaded. Available values are: • Null: (Default) Specifies that the PKCS#12 identity certificate download is disabled. • 0–255 characters.
PKCS12_PASSWD_RETRY	3	Specifies the number of attempts allowed for password entry. Available values are: • 3: (Default) • 0–100
PLAY_TONE_UNTIL_RTP	1	Specifies whether locally-generated ringback tone stops as soon as SDP is received for an early media session, or whether it will continue until RTP is actually received from the far-end party. Value Operation • 0: Stop ringback tone as soon as SDP is received. • 1: Continue ringback tone until RTP is received (default).
POE_CONS_SUPPORT		Enables power over Ethernet conservation mode. Value Operation • 0: Power conservation mode is not supported. • 1: Power conservation mode is supported.

Table continues…

Parameter name	Default value	Description
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 • 2: Prompt. The phone directly prompts the user to allow or deny the watcher's request. This parameter is not supported in IP Office environment as presence is not supported.
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.
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_EDITED_DIALING	2	Specifies the control for edited dialing.

Table continues…

Parameter name	Default value	Description
		Value Operation • 0: **Dialing Options** is not displayed. Edit dialing is disabled. The user cannot change edit dialing and the phone defaults to on-hook dialing. • 1: **Dialing Options** is not displayed. On hook dialing is disabled. The user cannot change edit dialing and the phone defaults to edit dialing. • 2: **Dialing Options** is displayed (default). The user can change edit dialing and the phone defaults to on-hook dialing. • 3: Dialing Options is displayed. The user can change edit dialing and the phone defaults to edit dialing.
PROVIDE_KEY_REPEAT_DELAY	0	Specifies how long a navigation button must be held down before it begins to auto-repeat, and if an option is provided by which the user can change this value. Value Operation • 0: Default (500ms) with user option (default). • 1: Short (250ms) with user option. • 2: Long (1000ms) with user option. • 3: Very Long (2000ms) with user option. • 4: No Repeat with user option. • 5: Default (500ms) without user option. • 6: Short (250ms) without user option. • 7: Long (1000ms) without user option. • 8: Very Long (2000ms) without user option. • 9: No Repeat without user option.
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.

Table continues…

Parameter name	Default value	Description
		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 (default 0)
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.
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 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.

Table continues…

Parameter name	Default value	Description
		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). • 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.

Table continues…

Parameter name	Default value	Description
		• 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. Valid values are 10 through 36000.
REDIRECT_TONE	1	Specifies the tone to play when a call goes to coverage. Valid values are 1-4.
REGISTERWAIT	900	Specifies the number of seconds between re-registrations with the current server.
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.

Table continues…

Parameter name	Default value	Description
		Values are separated by commas without any intervening spaces. Each value consists of a display name followed by an equals sign followed by a file name or URL. Display names can contain spaces, but if any do, the entire list must be quoted. Ring tone files must be single-channel WAV files coded in ITU-T G.711 u-law or A-law PCM with 8-bit samples at 8kHz.
RINGTONES_UPDATE	0	Specifies if the phone queries the file server to determine if there is an updated version of each custom ring tone file each time the phone starts up or resets. Value Operation 0: Phone only tries to download ring tones with new display names (default) 1: Phone checks for updated version of each ring tone file at startup
RINGTONESTYLE	0	Specifies the style of ring tones that are offered to the user for personalized ringing when **Classic** is selected, as opposed to **Rich**. Value Operation • 0: North American ring tones are offered (default). • 1: European ring tones are offered.
RTCP_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 Operations • 0: No • 1: Yes
RTCPCONT		Specifies if the sending of RTCP is enabled. • 0: No • 1: Yes
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.

Table continues…

Parameter name	Default value	Description
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 `challengePassword` 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 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.
SDPCAPNEG	1	Specifies if SDP capability negotiation is enabled. Value Operation 0: SDP capability negotiation is disabled. 1: SDP capability negotiation is enabled (default).
SEND_DTMF_TYPE	2	Specifies if DTMF tones are sent in-band as regular audio, or out-of-band using RFC 2833 procedures. Value Operation

Table continues…

Parameter name	Default value	Description
		1: in-band 2: out-of-band (default)
SERVER_CERT_RECHECK_HOURS	24	Specifies the time interval in hours for rechecking expiration and revocation status of the certificates that were used to establish any existing TLS connections. The valid range is from 0 to 32767.
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. **Note:** This parameter is set to 2 in IP Office environment.
SIP_CONTROLLER_LIST		
SIPCONFERENCECONTINUE	0	Specifies if a conference call continues after the host hangs up. Value Operation 0: Drop all parties (default) 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.
SIPPROXYSRVR	Null	Specifies a list of addresses of SIP proxy 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.
SIPREGPROXYPOLICY		Specifies if the phone attempts to maintain one or multiple simultaneous registrations. Value Operation

Table continues…

Parameter name	Default value	Description
		Alternate: Only a single registration is attempted and maintained. Simultaneous: Simultaneous registrations is attempted and maintained with all available controllers.
SIPSIGNAL	2	Specifies the type of transport used for SIP signaling. Value Operation 0: UDP 1: TCP 2: TLS (default)
SKINS		Specifies a list of tuples describing color scheme and layout used in phone display. Valid values are in a range of 0 to 1023 ASCII characters.
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 (default) 1: Enabled 2: Controlled from admin menu
SLMPERF	1	Specifies whether the SLA Monitor agent is enabled for phone performance monitoring. Value Operation 0: Disabled (default) 1: Enabled

Table continues…

Parameter name	Default value	Description
SLMPORT	50011	Specifies the UDP port that will be opened by the SLA Monitor agent to receive discovery and test request messages. Valid values are 6000 through 65535. The default value is 50011. **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
SLMSTAT	0	Specifies if the SLA Monitor agent is enabled or not. Value Operation 0: Disabled (default)

Table continues…

Parameter name	Default value	Description
		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.
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.
SP_DIRSRVR	Null	Sets the IP address or Fully-Qualified Domain Name (FQDN) of the LDAP Directory Server. Valid values are zero or more IP addresses in dotted-decimal or DNS format, separated by commas without intervening spaces, to a maximum of 255 ASCII characters. The default is null.
SP_DIRSRVRPORT	389	Sets the TCP port number of the LDAP Directory Server. The default port number is 389.
SP_DIRTOPDN	Null	Sets the Directory Topmost Distinguished Name. This value must be set to a non-null value to enable the LDAP application. The default is null, but DIRTOPDN should be set to the LDAP root entry.
SPEAKERSTAT	2	Specifies the operation of the speakerphone. Value Operation 0: Speakerphone disabled 1: One-way speaker (also called monitor) enabled.

Table continues…

Parameter name	Default value	Description
		2: Full (two-way) speakerphone enabled.
SSH_ALLOWED	0	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.
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.

Table continues…

Parameter name	Default value	Description
SUBSCRIBELIST	Null	Specifies a list of URIs to which the phone will send a subscribe message after the phone successfully registers with a call server, or when a subscribe push request is received with a type attribute all. The message is an HTTP GET for the URI with the phone's MAC address, extension number, IP address and model number appended as query values) The list can contain up to 255 characters. Values are separated by commas without any intervening spaces. If the value is set to null, subscribe messages are not sent.
SYMMETRIC_RTP	1	Specifies if the phone must discard received RTP or SRTP datagrams if their UDP source port number is not the same as the UDP destination port number included in the RTP or SRTP datagrams of that endpoint. Value Operation 0: Ignore the UDP source port number in received RTP/SRTP datagrams. 1: Discard received RTP/SRTP datagrams (default).
SNTP_SYNC_INTERVAL	1440	Specifies the time interval in minutes when the phone attempts to synchronize its time with the configured NTP servers. Valid values are from 60 min. to 2880 min.
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_STATUS	1	Specifies if the phone sends TCP keep alive messages. Value Operation 0: Keep-alive messages are not sent

Table continues…

Parameter name	Default value	Description
		1: Keep-alive messages are sent (default)
TIMEFORMAT		Specifies the format for time displayed in the phone. Value Operation 0: AM or PM format 1: 24h format
TLS_VERSION	0	Specifies the TLS version used for all TLS connections (except SLA monitor agent) Value Operation 0: TLS versions 1.0 and 1.2 are supported. 1: TLS version 1.2 only is supported.
TLSSRVRID	1	Specifies to validate the identity before the TLS handshake. Value Operation 0: Disabled. 1: Enabled.
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_QUAD_ZEROES_FOR_HOLD		Specifies the method to use to indicate that a call is on hold. Value Operation 1: For 0.0.0.0 IP address. Useful for compatibility with 3rd party SIP endpoints. 0: For a= directional attributes

Table continues…

Parameter name	Default value	Description
USBPOWER	2	Specifies that whether the power provided to the USB interface is controlled. Value Operation: • 0: Turn off USB power regardless of power source. • 1: Turn on USB power only if Aux powered. • 2: Turn on USB power regardless of power source. • 3: Turn on USB power if Aux powered or PoE Class 3 power.
V		
VLANSEPMODE	1	Specifies whether VLAN separation is enabled or disabled. 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.

Table continues…

Parameter name	Default value	Description
		Valid values are 2 through 900. The default value is 2.
VU_MODE	0	Specifies visiting user mode capabilities. Value Operation 0: No visiting user support. 1: User is prompted at registration time as to whether or not they are visiting. 2: Only visiting user registrations are allowed.
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.
WBCSTAT	1	Specifies whether a wideband codec indication is displayed when a wideband codec is used. Value Operation 0: Disabled 1: Enabled
WEBLMSRVR	Null	Sets the IP address or Fully-Qualified Domain Name (FQDN) of the licensing server. Valid values are zero or more IP addresses in dotted-decimal or DNS format, separated by commas without intervening spaces, to a maximum of 255 ASCII characters.

Index

Numerics

A

B

C

D

E

F

T

U

V