Installing and Administering Avaya J169/ J179 IP Phone

Release 1.5
Issue 2
July 2018

Note

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

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

Copyright

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, 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

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

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

Japan Statements

Class B Statement

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

この装置は、クラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。　　　　　ＶＣＣＩ－Ｂ

Denan Power Cord Statement

⚠ **Danger:**

Please be careful of the following while installing the equipment:

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

⚠ **警告**

本製品を安全にご使用頂くため、以下のことにご注意ください。

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

México Statement

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

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

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

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

Power over Ethernet (PoE) Statement

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

U.S. Federal Communications Commission (FCC) Statements

Compliance Statement

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

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

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

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

When using IEEE 802.11a wireless LAN, this product is restricted to indoor use, due to its operation in the 5.15 to 5.25GHz frequency range. The FCC requires this product to be used indoors for the frequency range of 5.15 to 5.25GHz to reduce the potential for harmful interference to co channel mobile satellite systems. High-power radar is allocated as the primary user of the 5.25 to 5.35GHz and 5.65 to 5.85GHz bands. These radar stations can cause interference with and/or damage to this device.

Class B Part 15 Statement

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

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 when installed complies with the essential requirements and other relevant provisions of the EMC Directive 2014/30/EU, Safety LV Directive 2014/35/EU, and Radio Equipment Directive 2014/53/EU. A copy of the Declaration may be obtained from http://support.avaya.com or Avaya Inc., 4655 Great America Parkway, Santa Clara, CA 95054–1233 USA.

WiFi and BT transmitter

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

General Safety Warning

- Use only the Avaya approved Limited Power Source power supplies specified for this product.
- Ensure that you:
    - Do not operate the device near water.
    - Do not use the device during a lightning storm.
    - Do not report a gas leak while in the vicinity of the leak.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

Contents

Chapter 1: Introduction

Purpose

This document contains information about preparing Avaya J100 Series IP Phones for installation, deployment, initial administration, and administration tasks including data and security.

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

The deployment engineers or the support personnel must have the following knowledge, skills, and tools:

Knowledge

- DHCP
- SIP
- Configuring 802.1x and VLAN

Skills

How to administer and configure:

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

Chapter 2: Avaya J169/179 IP Phone Overview

Phone overview

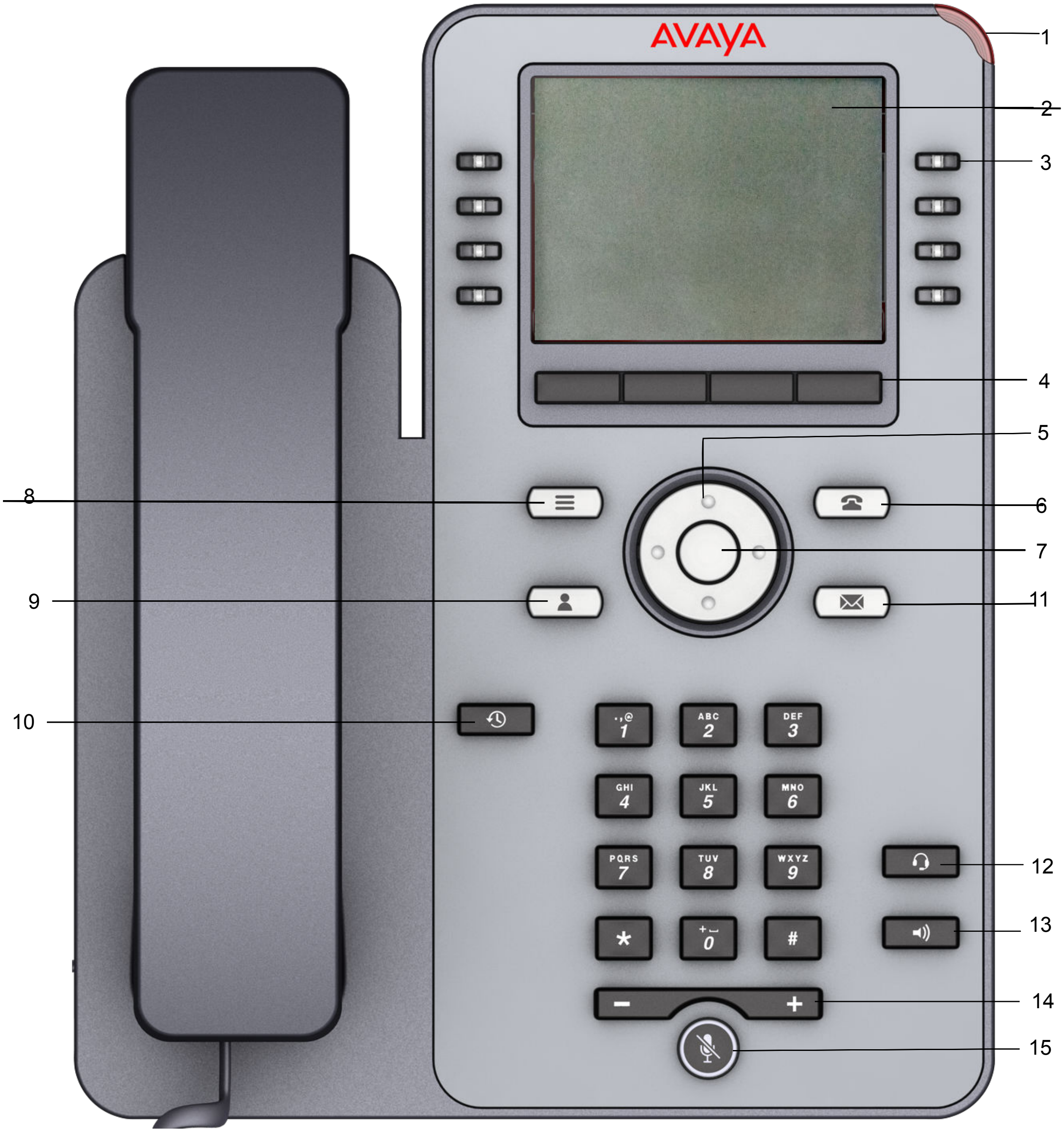
The Avaya J169/J179 IP Phone is a SIP-based phone, intended to be used for business communications. The phone supports eight call appearances with four lines of call display. The phone can support up to three button modules, and each button module supports 24 call appearances.

The Avaya J169 IP Phone has a grayscale display, and the Avaya J179 IP Phone has a color display.

Physical specifications

- Eight call appearances
- A 128 x 32 pixels graphical LCD
- Four softkeys
- Dual 10/100/1000 network ports
- Optional 5V DC Power support
- 48V GSPPOE power adapter support
- Up to three button module support

Physical layout



No.	Name	Description
1	Beacon LED	Displays a red light for the following visual alerts: • Incoming call • Voice mail and messages
2	Phone display	Displays two areas: 1. Top Bar: It is always visible, and displays communication status, time and date, and device status. 2. Application area displays the following: • Application header: It displays the context specific application title, and one or more subtitles. The header is always empty on the Phone screen. • Application content area: It displays menus, lists, pop-up windows, images, or other application content. • Softkey labels area: It displays labels with information about the state of the **Soft Keys** button.
3	Line Keys	Used to select the corresponding rows. Each line key has a LED that displays the following visual alerts: • Red light: Disabled features. • Green light: Incoming call and enabled features. • Red and Green light: Phone is off-hook.
4	Soft Keys	Used to select the corresponding label of context-specific actions. With the **Help** soft key, you can view a short description of the features available on your phone. The administrator must activate the Help feature.
5, 7	Navigation cluster	Used to navigate on the phone screen. • **Up** and **Down** arrow keys: To scroll up and down. • **Right** and **Left** arrow keys: To move cursor in the text input field, and to toggle values in the selection fields. • **OK** button: To select the action assigned to the first soft key.
11	Voicemail	Used to dial the configured voice mail number to receive a voice message.
12	Headset	Used to toggle your call from the speaker to headset.
13	Speaker	Used to turn on the speaker.
14	Volume	Used to adjust volume of a handset, speaker, or ringtone. • (**+**) : To increases the volume. • (**-**): To decrease the volume.
15	Mute Button	Used to mute and unmute the outgoing audio.

Application keys provide direct access to the corresponding applications.

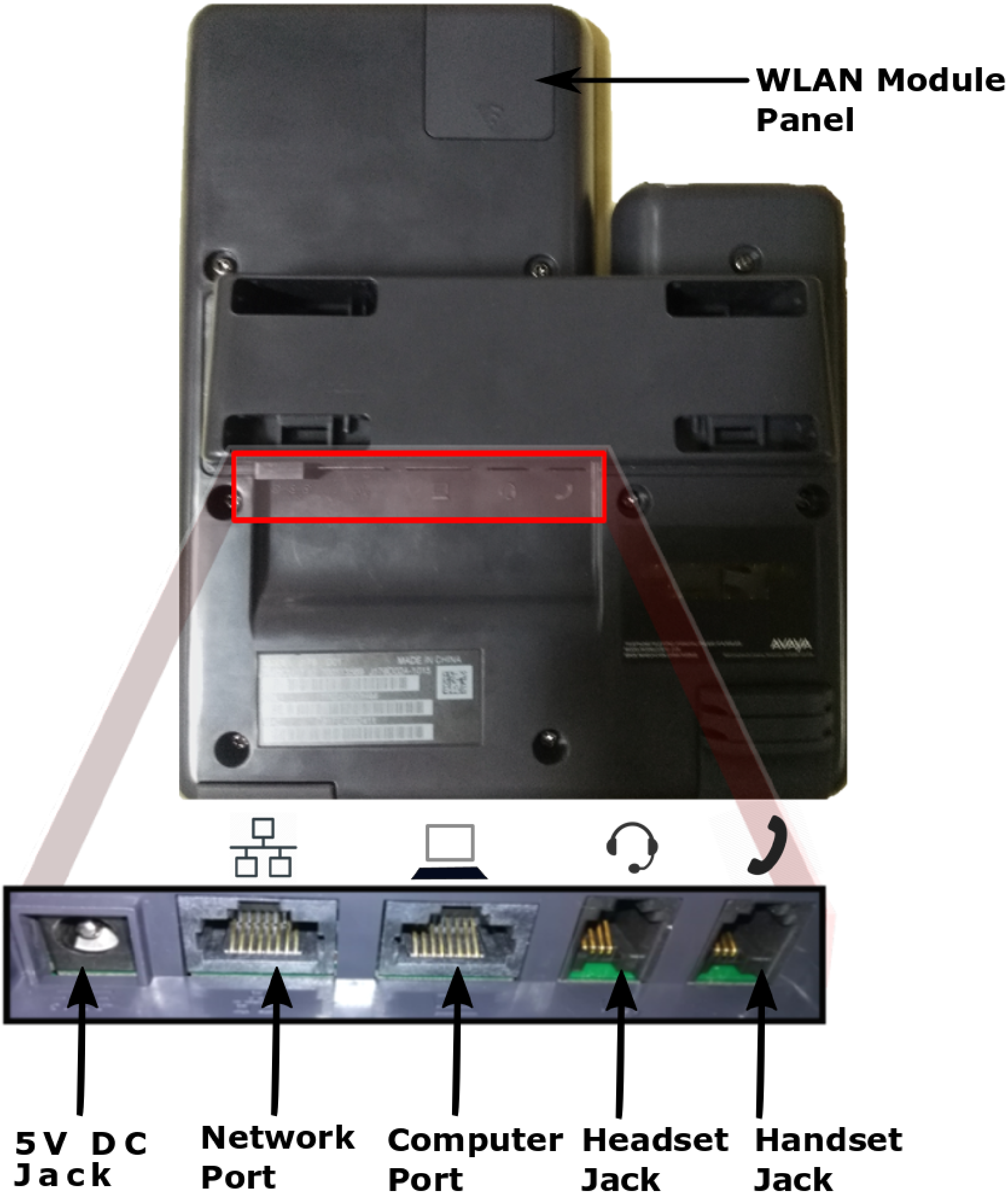
No.	Application keys	Description
6	Phone key	Displays the phone screen.
8	Main Menu	Displays a list of options, such as Features, Applications, Settings, and Network Information.
9	Contacts	Displays the entries in your contact list.
10	Recents	Displays all call history list.

Connection Jacks

The following image illustrates the connection jacks that are present on the back panel of Avaya J169/J179 IP Phone.

Note:

The image schematically describes which device to connect to which jack.


WLAN Module Panel
5V DC Jack
Network Port
Computer Port
Headset Jack
Handset Jack

Optional components

You can use the following optional components with phone:

- 5 VDC Power adapter
- Button module (JBM24)
- J100 Wireless Module
- GSPPOE - Avaya 48V PoE power inserter

Power management

Avaya J169/J179 IP Phone receives power from the following sources:

- Avaya DC 5 volt power adapter with barrel jack
- 802.3af PoE (Class 1)
- 802.3af PoE (Class 2) if using JBM24 or J100 Wireless Module or both
- GSPPOE - Avaya 48V PoE power inserter

The Avaya DC 5 volt power adapter supports all accessories of Avaya J169/J179 IP Phone. If the phone is connected to a power adapter and a PoE cable, the power adapter takes precedence over PoE.

If the power adapter is disconnected and the PoE cable is still connected, the phone reboots and continues to work on PoE.

If Avaya J169/J179 IP Phone is connected to a PoE cable, and the power adapter is connected, the phone continues to work without a reboot.

Chapter 3: Initial setup and connectivity

This chapter describes about the prerequisites and the initial setup of the Avaya J100 Series IP Phones. It also describes the procedure to connect the phone to the enterprise network for the first time.

Initial setup checklist

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

No.	Task	Reference	✔
1	Check the prerequisites.	See Hardware and software prerequisites on page 16 for more information.	
2	Configure system manager user profile.	See Avaya Aura System Manager user profile worksheet on page 17 for more information.	
3	Configure the servers.	See Server configuration on page 28 for more information.	
5	Configure LLDP.	See Configuration through LLDP on page 35 for more information.	
6	Configure VLAN.	See Virtual LAN (VLAN) overview on page 45 for more information.	
9	Install the phone.	See Installing the phone on page 22 for more information.	

Hardware and software prerequisites

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

Hardware prerequisites

Ensure that the LAN:

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

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

Software prerequisites

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

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

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

Avaya Aura® System Manager user profile worksheet

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

Data for	Field	Value	Notes
System Manager User Profile			
Identity tab			

Table continues…

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

Table continues…

Data for	Field	Value	Notes
	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*.

Diagram: IP phone setup

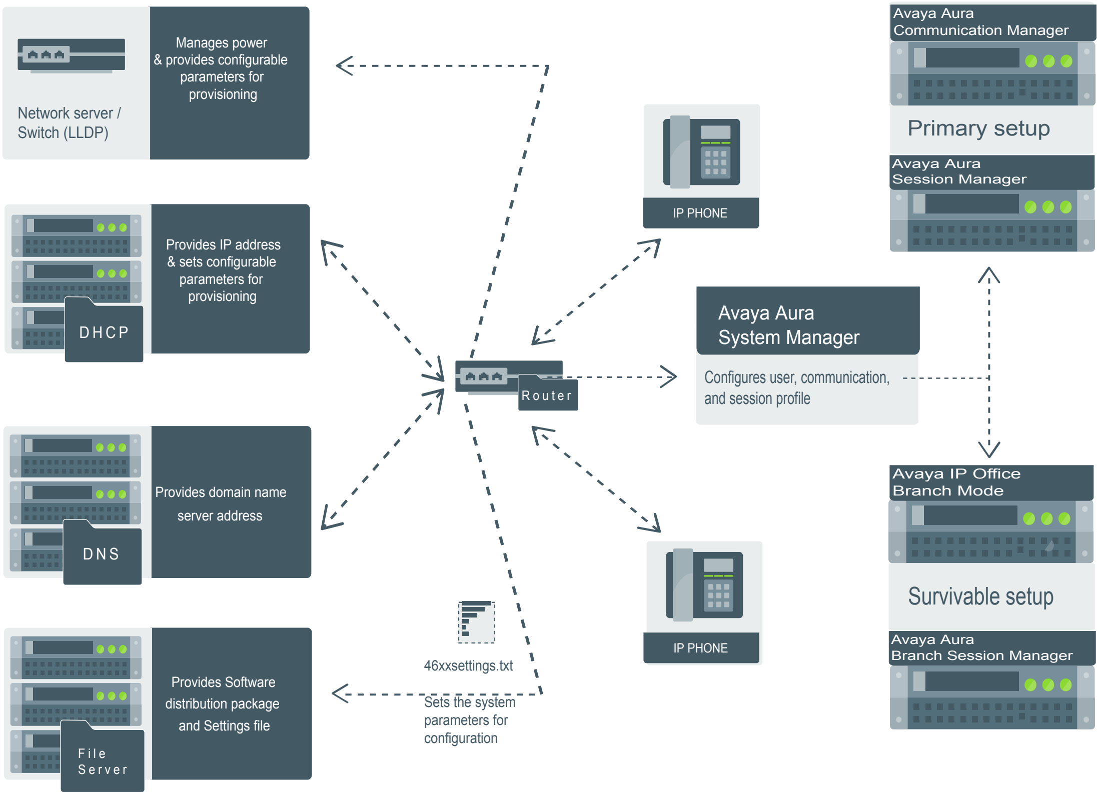
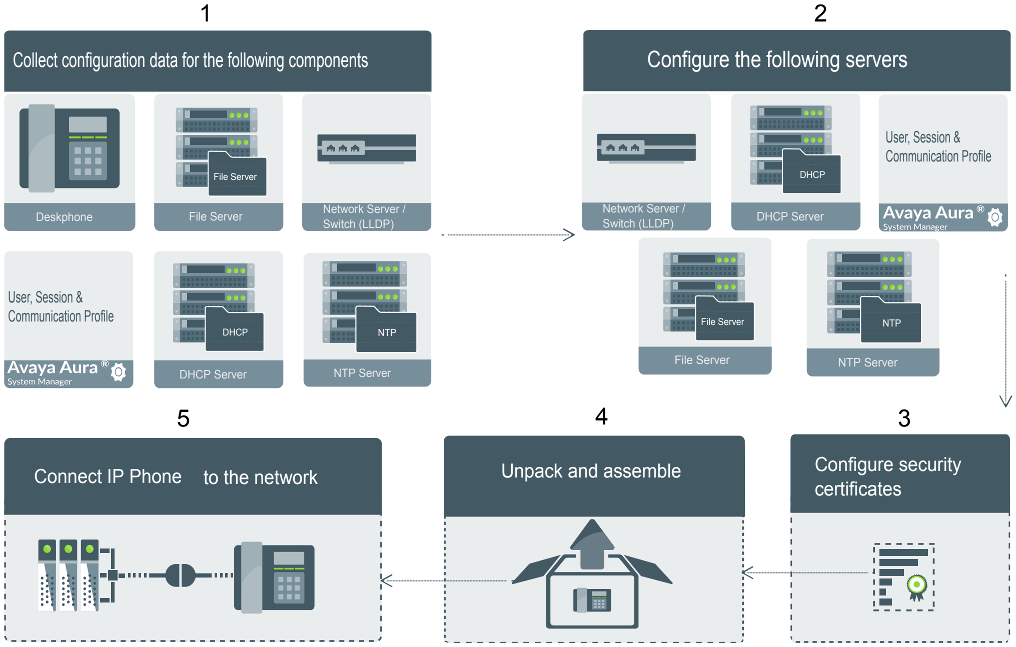

Network server /
Switch (LLDP)
Manages power & provides configurable parameters for provisioning
DHCP
Provides IP address & sets configurable parameters for provisioning
DNS
Provides domain name server address
File Server
Provides Software distribution package and Settings file
46xxsettings.txt
Sets the system parameters for configuration
Router
IP PHONE
IP PHONE
Avaya Aura System Manager
Configures user, communication, and session profile
Avaya Aura Communication Manager
Primary setup
Avaya Aura Session Manager
Avaya IP Office Branch Mode
Survivable setup
Avaya Aura Branch Session Manager

Diagram: phone deployment process


1
Collect configuration data for the following components
Deskphone
File Server
File Server
Network Server / Switch (LLDP)
User, Session & Communication Profile
Avaya Aura® System Manager
DHCP
DHCP Server
NTP
NTP Server
2
Configure the following servers
Network Server / Switch (LLDP)
DHCP
DHCP Server
User, Session & Communication Profile
Avaya Aura® System Manager
File Server
File Server
NTP
NTP Server
3
Configure security certificates
4
Unpack and assemble
5
Connect IP Phone to the network

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	—	✔	✔	✔	✔

Table continues…

Method	Can administer				
Avaya Aura® System Manager and IP Office	—	—	—	—	✔
Administration menu on the phone	✔	✔	—	—	✔
Web UI	✔	✔	✔	✔	✔

Precedence of administration methods

Most of the parameters are configured through multiple methods. If you configure a parameter through more than one method, the device applies the settings of the method that has a higher precedence. The following list shows the precedence of the methods in the highest to lowest order:

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

Note:

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

Installing the phone

Before you begin

You must do the following:

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

Procedure

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

   The phone powers up and starts to initialize.
3. The initialization procedure consists of the following processes:
   a. The phone checks for LLDP messages.

   b. The phone sends a DHCP DISCOVER message to discover the DHCP server in the network and invokes the DHCP process.

      If the phone does not receive a provisioning server address from the configuration setup, the phone displays the Configure Provision Server screen.

   c. In the Configure Provision Server screen, press the **Config** softkey and enter the address of the provisioning server. The provisioning server address can be in the form of IP address or a Fully Qualified Domain Name (FQDN). To enter the dot symbol (.) in the field, press the alphanumeric softkey to toggle to the alphanumeric mode.

   d. The phone verifies the VLAN ID, and starts tagging the data and voice packets accordingly.

   e. The phone sends and identifies an upgrade script file, gets the `Settings` file, the language files, and any firmware updates.

      - If configured to use simple certificate enrollment protocol (SCEP), the phone downloads a valid device certificate.
      - The phone displays only the **Admin** softkey for 15 seconds, and then the **Admin** and the **Login** softkeys.

        Note:

        For subsequent restarts, if the user login is automatic and the supplied credentials are valid, the **Login** softkey is not displayed.
4. Do one of the following:
   - To access the user login screen, press the **Login** softkey.
   - To access the Admin menu, press the **Admin** softkey and enter the admin menu password.

Wall mounting Avaya J169/J179 IP Phone

About this task

The procedure describes about the wall mounting procedure for Avaya J169/J179 IP Phone with illustration as a reference.

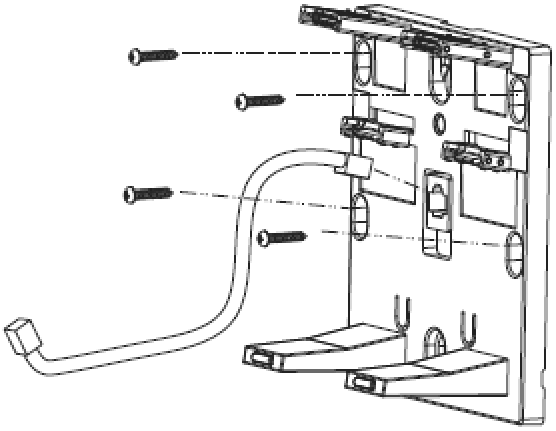
Before you begin

Get the following items:

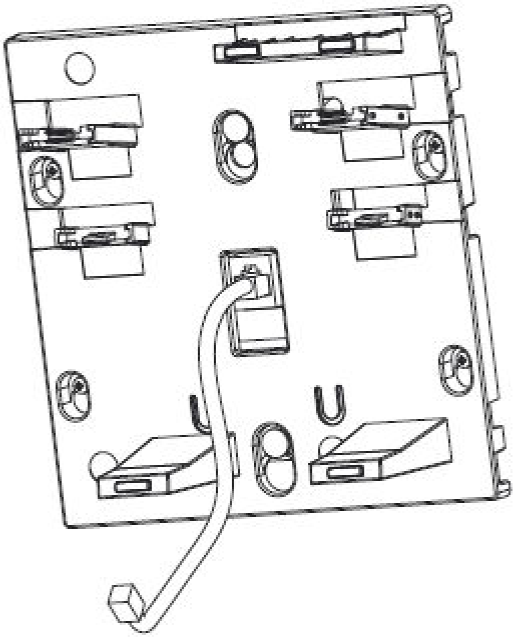
- Avaya J169/J179 IP Phone wall mounting kit that contains a wall mount bracket, and an Ethernet cable. The part number of the wall mount bracket is 700513631.
- Four #8 screws. The screws are not provided with the Avaya J169/J179 IP Phone wall mounting kit.

Procedure

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

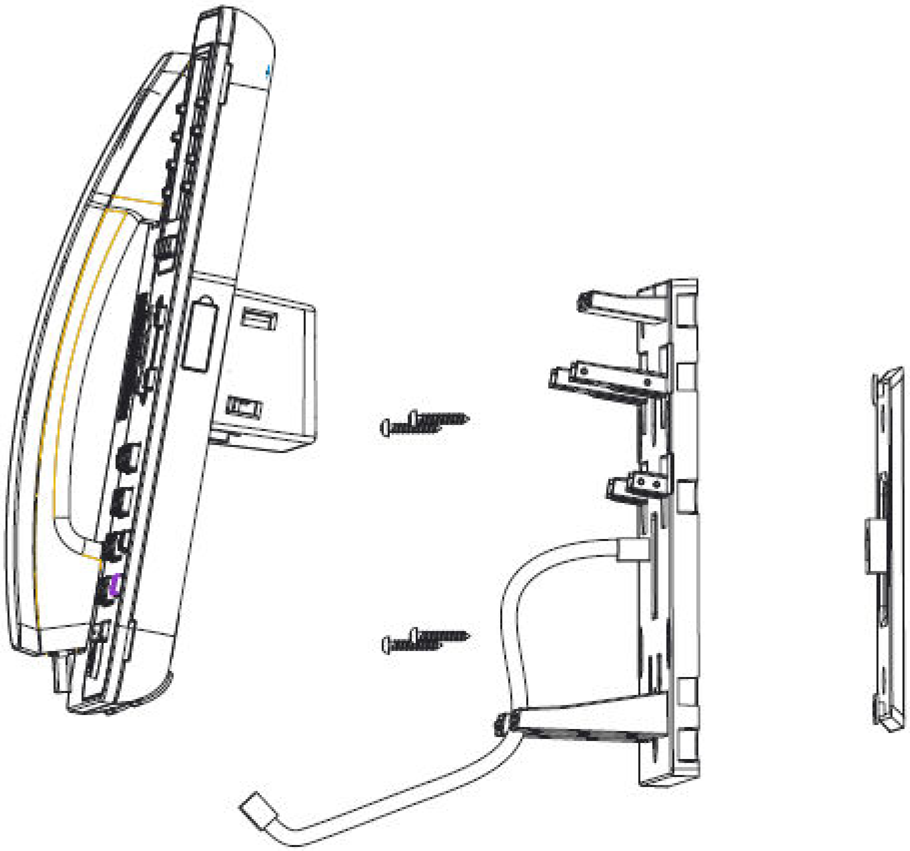
      

    - If there is a pre-installed wall plate, place the wall mount bracket over the wall plate. In this case, you do not need the screws.



2. Attach one end of the Ethernet cable to the 10/100 network port of the phone and the other end to the wall jack.
3. Attach the phone to the wall mount bracket by inserting the two upper tabs of the wall mount bracket into the slots on the back of the phone. The lower pair of tabs rest against

the back of the phone and ensure that the phone does not move when the keys are pressed.



Post installation checklist

To ensure that the phone is properly installed and running properly, verify that the following requirements are complete.

No.	Task	Reference	✔
1	Has the phone acquired an IP address?		

Table continues…

No.	**Task**	**Reference**	✔
2	Are you able to make a call from the phone?		
3	Are you able to perform backup-restore?		
3	Are you able to modify the phone's Settings file parameters and end user settings.	List of configuration parameters on page 95	
4	Are you able to upgrade your phone?	Upgrading the device on page 83	
5	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*	

Chapter 4: Configuring users, servers, and VLAN

Server configuration

To install Avaya J100 Series IP Phones, you must configure the following servers:

- HTTP or HTTPS File Server: To download and save the software distribution package and the settings file. Examples of a File Server:
    - Apache
    - Internet Information Services (IIS)
    - Avaya Utility Server
- DHCP server: To dynamically assign IP addresses and provide device configuration parameters.

Related links

File Server configuration on page 28
DHCP server configuration on page 35

File Server configuration

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

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

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

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

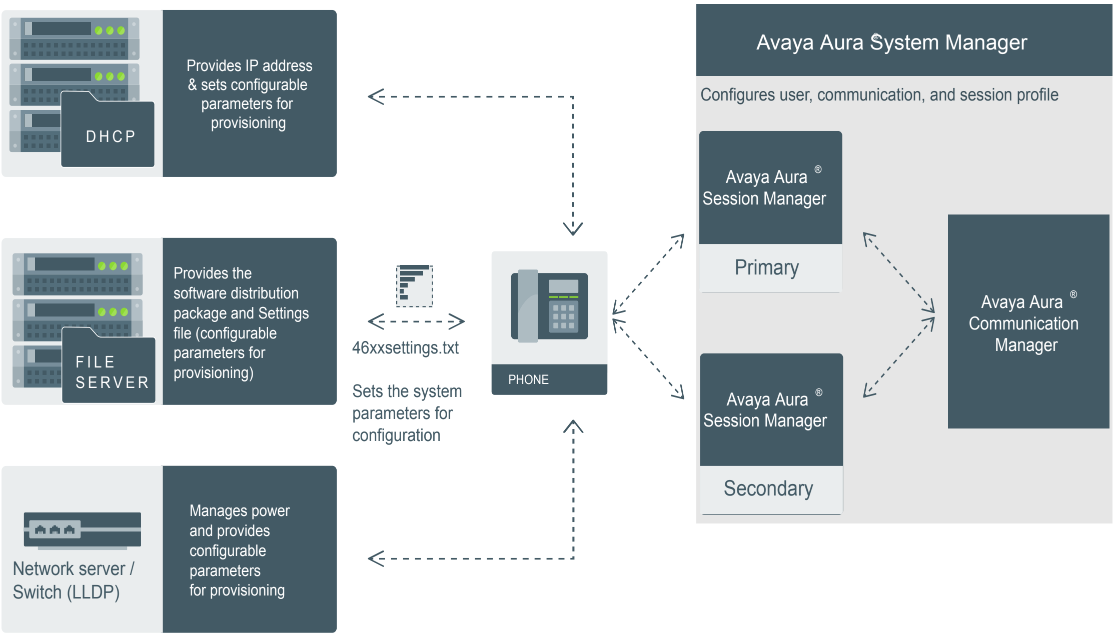

DHCP
Provides IP address & sets configurable parameters for provisioning
FILE SERVER
Provides the software distribution package and Settings file (configurable parameters for provisioning)
46xxsettings.txt
Sets the system parameters for configuration
PHONE
Network server / Switch (LLDP)
Manages power and provides configurable parameters for provisioning
Avaya Aura System Manager
Configures user, communication, and session profile
Avaya Aura ® Session Manager
Primary
Avaya Aura ® Session Manager
Secondary
Avaya Aura ® Communication Manager

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

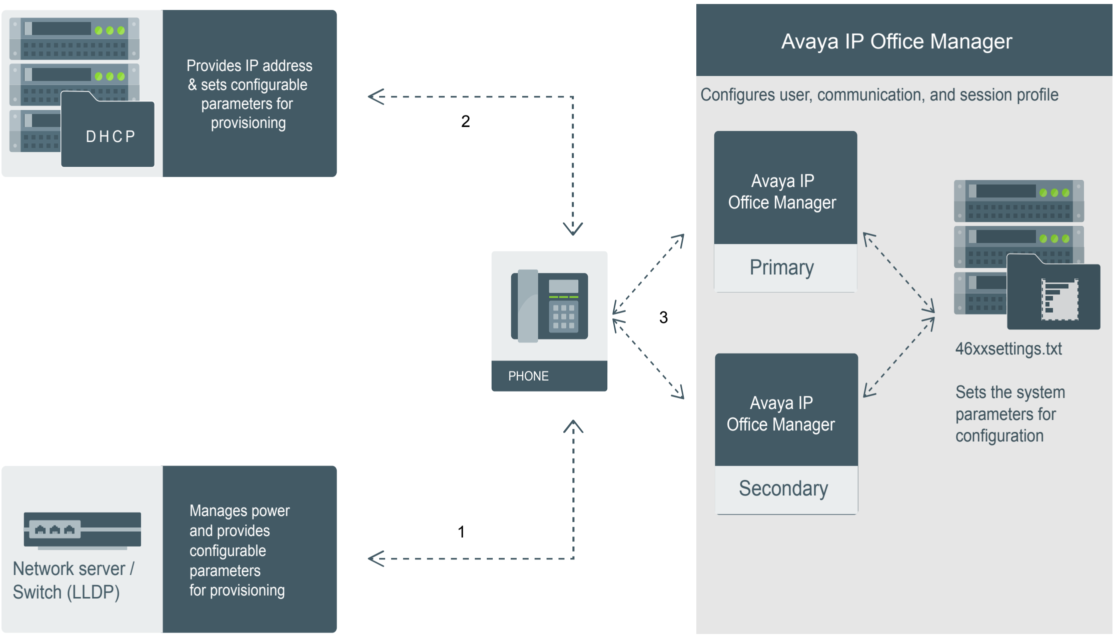

DHCP
Provides IP address & sets configurable parameters for provisioning
2
Avaya IP Office Manager
Configures user, communication, and session profile
Avaya IP Office Manager
Primary
3
PHONE
46xxsettings.txt
Sets the system parameters for configuration
Avaya IP Office Manager
Secondary
1
Network server / Switch (LLDP)
Manages power and provides configurable parameters for provisioning

Figure 2: Diagram: Phone setup in IP Office environment

Related links

Server configuration on page 28
Setting up a file server on page 30
Software distribution package on page 31
Downloading and saving the software on page 32
Contents of the settings file on page 32
Configuring the Settings file on page 34

Setting up a file server

About this task

Use this procedure to configure a file server. The file server is used to download and store distribution packages and settings files.

Procedure

1. Install the HTTP or HTTPS server according to the server vendor’s instruction.
2. Download the software distribution package and the 46xxsettings.txt settings file.
3. Extract the distribution package and save the extracted files and the 46xxsettings.txt settings file on the file server.

Related links

File Server configuration on page 28

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

File Server configuration on page 28

Downloading and saving the software

Before you begin

Ensure that your file server is set up.

Procedure

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

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

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

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

Related links

File Server configuration on page 28

Upgrading the device on page 83

Contents of the settings file

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

- Tags, which are lines that begin with a single "#" character, followed by a single space character, followed by a text string with no spaces.
- **Goto** commands, of the form **GOTO *tag.* Goto** commands cause the phone to continue interpreting the settings file at the next line after a **# *tag*** statement. If no such statement exists, the rest of the settings file is ignored.
- Conditionals, of the form **IF *$parameter_name* SEQ *string* GOTO *tag***. Conditionals cause the **Goto** command to be processed if the value of the parameter named ***parameter_name*** exactly matches ***string***. If no such parameter named ***parameter_name*** exists, the entire conditional is ignored. The only parameters that can be used in a conditional statement are: GROUP, MACADDR, MODEL and MODEL4.
- **SET** commands, of the form **SET *parameter_name value***. Invalid values cause the specified value to be ignored for the associated ***parameter_name*** so the default or previously

administered value is retained. All values must be text strings, if the value itself is numeric, you must place the numeric value inside a pair of quotation marks. For example, "192.x.y.z"

- Comments, which are statements with characters "**##**" in the first column.
- GET commands, of the form ***GET filename.*** The phone attempts to download the file named by ***filename***, and if it is successfully obtained, it will be interpreted as an additional settings file, and no additional lines will be interpreted in the original file. If the file cannot be obtained, the phone will continue to interpret the original file.

The Avaya-provided upgrade file includes a line that tells the phones to **GET *46xxsettings.txt***. This line cause the phone to use HTTP/HTTPS to attempt to download the file specified in the **GET** command. If the file is obtained, its contents are interpreted as an additional script file. That is how your settings are changed from the default settings. If the file cannot be obtained, the phone continues processing the upgrade script file. Also, if the settings file is successfully obtained but this does not change any settings, the phone continues to use HTTP.

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

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

Parameter	Retained
AGCHAND	Y
AGCHEAD	Y
AGCSPKR	Y
APPNAME	N
AUDIOENV	N
AUDIOSTHD	N
AUDIOSTHS	N
AUTH	Y
BAKLIGHTOFF	Y
CNGLABEL	Y
DAYLIGHT_SAVING_SET TING_MODE	Y
DHCPSTD	N
HEADSYS	N
HOMEIDLETIME	N
LOG_CATEGORY	Y
LOGSRVR	N
LOCAL_LOG_LEVEL	Y
LANG0STAT	Y
MSGNUM	N

Table continues…

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

Related links

File Server configuration on page 28

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 autogenerated 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 J100 Series IP Phones 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

File Server configuration on page 28

DHCP server configuration

Configure the DHCP server to:

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

Related links

Server configuration on page 28
Setting up a DHCP server on page 35

Setting up a DHCP server

Procedure

1. Install the DHCP server according to the DHCP server vendor's instructions.
2. Configure the available range of IP addresses.
3. Configure the required DHCP options.

Related links

DHCP server configuration on page 35

Configuration through LLDP

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

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

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

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

By using LLDP, you can configure the following:

- Call server IP address
- File server
- PHY2VLAN
- L2QVLAN and L2Q

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.

Table continues…

Category	TLV Name (Type)	TLV Info String (Value)
TIA LLDP MED	Inventory – Hardware Revision	MODEL - Full Model Name.
TIA LLDP MED	Inventory – Firmware Revision	Firmware version.
TIA LLDP MED	Inventory – Software Revision	Software version or filename.
TIA LLDP MED	Inventory – Serial Number	Device serial number.
TIA LLDP MED	Inventory – Manufacturer Name	Avaya.
TIA LLDP MED	Inventory – Model Name	MODEL with the final Dxxx characters removed.
Avaya Proprietary	Call Server IP address	Call Server IP Address. Subtype = 3.
Avaya Proprietary	IP Phone addresses	Phone IP address, Phone Address Mask, Gateway IP Address. Subtype = 4.
Avaya Proprietary	File Server	File Server IP Address. Subtype = 6.
Avaya Proprietary	802.1Q Framing	802.1Q Framing = 1 if tagging or 2 if not.
Basic Mandatory	End-of-LLDPDU	Not applicable.

TLV impact on system parameter values

System parameter name	TLV name	Impact
PHY2VLAN	IEEE 802.1 Port VLAN ID	The value of the PHY2VLAN parameter on the phone is configured from the value of the Port VLAN identifier in the TLV.
L2QVLAN and L2Q	IEEE 802.1 VLAN Name	The value is changed to the TLV VLAN Identifier. L2Q is set to 1 (ON). A check is made as to whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. VLAN Name TLV is ignored if: • The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0. • The current value of L2QVLAN was set by a TIA LLDP MED Network Policy TLV.

Table continues…

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

Table continues…

System parameter name	TLV name	Impact
L2Q	Proprietary 802.1 Q Framing	If the value of TLV = 1, L2Q is set to 1 (On). If the value of TLV = 2, L2Q is set to 2 (Off). If the value of TLV = 3, L2Q is set to 0 (Auto). A check is made as to whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. This TLV is ignored if: • The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0. • The current L2QVLAN value was set by an IEEE 802.1 VLAN name. • The current L2QVLAN value was set by a TIA LLDP MED Network Policy (Voice) TLV.

Configuration through DHCP

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

- Avaya Aura® Session Manager address.
- IP address
- Subnet mask
- IP address of the router
- IP address of the HTTP or HTTPS file server
- IP address of the SNTP server
- IP address of DNS

You can configure the DHCP server to:

- Dynamically assign IP addresses to the .
- Provision device and site-specific configuration parameters through various DHCP options.

DHCP Site Specific Option

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

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

Following parameters can be configured with this feature:

Parameter	Description
ADMIN_PASS WORD	Specifies the security string used to access local procedures. The default is 27238. This is meant to replace PROCPSWD as it provides a more secure password syntax.
HTTPDIR	Specifies the path to prepend to all configurations and data files the device might request when starting up, that is, the path, relative to the root of the HTTP file server, to the directory in which the device configuration and date files are stored. The path may contain no more than 127 characters and may contain no spaces. HTTPDIR is the path for all HTTP operations. The command is `SET HTTPDIR=<path>`. In configurations where the upgrade and binary files are in the default directory on the HTTP server, do not use the `HTTPDIR=<path>`.
HTTPPORT	Sets the TCP port used for HTTP file downloads from non-Avaya servers. The default is 80.
HTTPSRVR	IP addresses or DNS names of HTTP file servers used for downloading settings, language, and firmware files during startup. The firmware files are digitally signed, so TLS is not required for security.
ICMPDU	Controls the extent to which ICMP Destination Unreachable messages are sent in response to messages sent to closed ports so as not to reveal information to potential hackers. The default is 1, that is sends Destination Unreachable messages for closed ports used by traceroute.
ICMPRED	Controls whether ICMP Redirect messages are processed. The default is 0, that is, redirect messages are not processed.
L2Q	802.1Q tagging mode. The default is 0 for automatic.
L2QVLAN	VLAN ID of the voice VLAN. The default is 0.
PHY1STAT	Specifies the speed and duplex settings for the Ethernet line interface. The default value is 1 for auto-negotiate.
PHY2STAT	Specifies the speed and duplex settings for the secondary (PC) Ethernet interface. The default value is 1.
PROCPSWD	Security string used to access local procedures. The default is 27238. ADMIN_PASSWORD replaces this parameter if ADMIN_PASSWORD is set in the `46xxsettings.txt` file.
REUSETIME	Time in seconds for IP address reuse timeout, in seconds. The default is 60 seconds.
SIP_CONTROL LER_LIST	SIP proxy or registrar server IP or DNS addresses that can be 0 to 255 characters, IP address in the dotted decimal name format, separated by commas and without any intervening spaces. The default is null, that is, no controllers.

Table continues…

Parameter	Description
TLSDIR	Used as path name that is prepended to all file names used in HTTPS GET operations during initialization. The string length can be from 0 to 127.
TLSPORT	Destination TCP port used for requests to https server in the range of 0 to 65535. The default is 443, the standard HTTPS port.
TLSSRVR	IP addresses or DNS names of Avaya file servers used to download configuration files. Firmware files can also be downloaded using HTTPS. **Note:** Transport Layer Security is used to authenticate the server.
VLANTEST	Number of seconds to wait for a DHCPOFFER on a non-zero VLAN. The default is 60 seconds.

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

DHCP options

You can configure the following options in the DHCP server:

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

Table continues…

Option	Description
	- 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. The value 6889 is an Avaya enterprise number. All values are interpreted as strings of ASCII characters that are accepted with or without a null termination character. Any invalid value is ignored and the corresponding parameter value is not set.
Option 51	Specifies the DHCP lease time. If this option is not received, the DHCPOFFER is not accepted. Assign a lease time of six weeks or greater. If this option has a value of FFFFFFFF hex, the IP address lease is assumed to be infinite, so that the renewal and rebinding procedures are not necessary even if options 58 and 59 are received. Expired leases causes the device to reboot.
Option 52	Specifies the overload option. If this option is received in a message, the device interprets the sname and file parameters.
Option 53	Specifies the DHCP message type. The value can be one of the following: • 1 for DHCPDISCOVER • 3 for DHCPREQUEST For DHCPREQUEST sent to renew the device IP address lease: • If a DHCPACK is received in response, a log event record is generated with a Log Category of DHCP.

Table continues…

Option	Description
	• 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

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

Table continues…

Code	Parameter
10	L2QVLAN
11	PHY1STAT
12	PHY2STAT
14	SIG
15	SIP_CONTROLLER_LIST

Extending use of DHCP lease

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

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

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

Parameter configuration through DHCP

Parameter	Set to
DHCP lease time	Option 51, if received
DHCP lease renew time	Option 58, if received
DHCP lease rebind time	Option 59, if received

Table continues…

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

Virtual LAN (VLAN) overview

VLANs provide a means to segregate your network into distinct groups or domains. They also provide a means to prioritize the network traffic into each of these distinct domains. For example, a network may have a Voice VLAN and a Data VLAN. Grouping devices that have a set of common requirements 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.

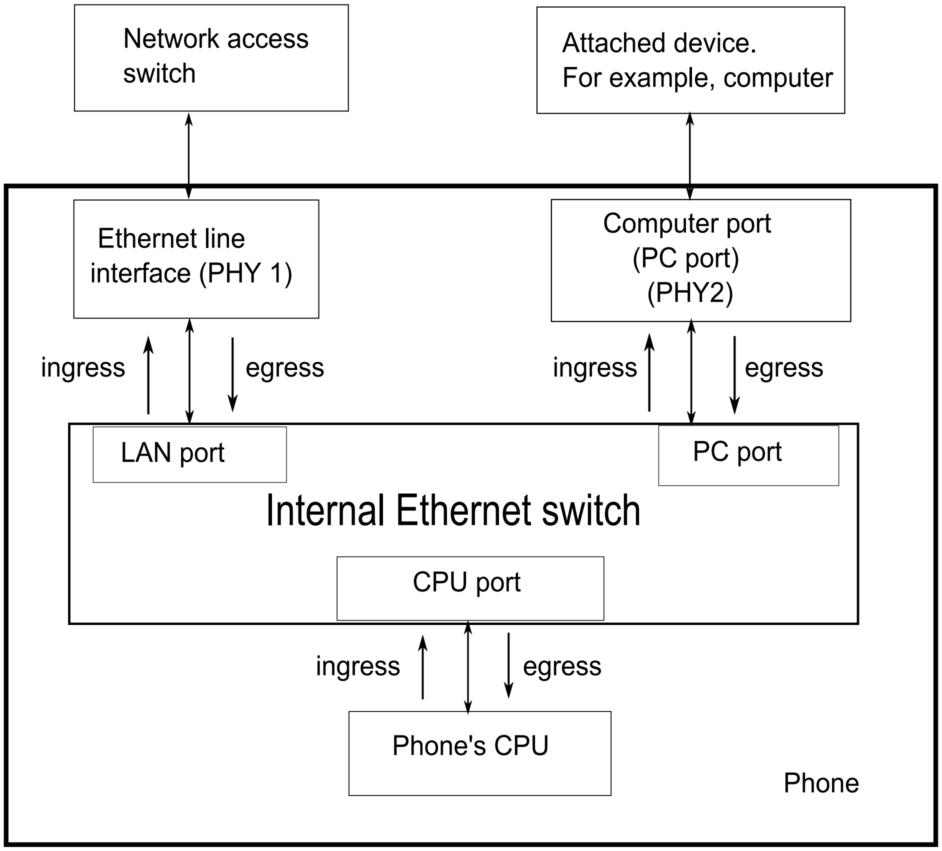
Related links

VLAN separation on page 45
External switch configuration on page 48
Exceptions to the VLAN forwarding rules on page 49
Special considerations on page 49
VLAN parameters on page 50

VLAN separation

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

The configuration of the internal switch of the phone can be done through the `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

Related links

Virtual LAN (VLAN) overview on page 45

VLAN separation modes on page 48

VLAN separation modes

Avaya J100 Series IP Phones supports two VLAN separation modes:

- No VLAN separation mode: In this mode the CPU port of the port receives untagged frames and tagged VLAN frames on any VLAN irrespective of whether the phone sends untagged frames or tagged frames. This traffic can be received from the PC port or LAN port. The filtering of the frames is done by the CPU itself. In order to reduce unnecessary traffic to the CPU, the administrator should configure only the necessary VLANs on the external switch port, in particular, voice VLAN and data VLAN.
- Full VLAN separation mode: This is the default mode. In this mode the CPU port of the phone receives tagged frames with VLAN ID = L2QVLAN whether they are from the LAN port or 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 J100 Series IP Phones to work in this mode all the following conditions must be met:
    - VLANSEPMODE = 1 (default)
    - L2Q = 0 (auto, default) or 1 (tag)
    - L2QVLAN is not equal to 0
    - PHY2VLAN is not equal to 0
    - L2QVLAN is not equal to PHY2VLAN
    - The phone actually sends tagged VLAN frames. This means that the DHCP server on voice VLAN (L2QVLAN) is reachable and the phone receives IP address on voice VLAN.

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

Note:

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

Related links

VLAN separation on page 45

External switch configuration

Configure the following for the external switch port:

- Bind VLAN to the voice VLAN (L2QVLAN) and the data VLAN (PHY2VLAN). It is important to restrict the VLAN binding when in No VLAN separation mode. This is because there is no filtering by the internal phone switch and the CPU of the phone is subject to all the traffic going through the phone. When in Full VLAN separation mode, the internal phone switch will filter any tagged VLAN frames with VLANs other than voice VLAN (L2QVLAN) and data VLAN (PHY2VLAN) in any case. However, you must configure only the necessary VLANs on the external switch port.

- Set the default VLAN as the data VLAN (PHY2VLAN). This is the VLAN assigned by the external switch port to untagged frames received from phone LAN port.
- Configure one of the following for egress tagging:
  - Data VLAN is untagged and voice VLAN is tagged.
  - Data VLAN and voice VLAN are both tagged. You must configure this option to have Full VLAN separation.

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

Related links

Virtual LAN (VLAN) overview on page 45

Exceptions to the VLAN forwarding rules

Exceptions to the VLAN forwarding rules are as follows:

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

Related links

Virtual LAN (VLAN) overview on page 45

Special considerations

Special use of VLAN ID=0

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

Automatic failback of VLAN tagging

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

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

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

VLAN support on the computer or PC port

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

Related links

Virtual LAN (VLAN) overview on page 45

VLAN parameters

The following configuration parameters are used to configure VLAN functionality on the network switch internal to the phone.

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

Table continues…

Parameter name	Default value	Description
		• DHCP option 43 • LLDP
VLANTEST	60	Specifies the number of seconds that the phone waits prior to failing back to a different VLAN ID if no response is received from the DHCP server. Valid values are 0 through 999. Value operation: • 0: The phone continues to attempt a DHCP REQUEST forever. VLANTEST is configured through: • `Settings` file • A name equal to value pair in DHCPACK message
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

Table continues…

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

Related links

Virtual LAN (VLAN) overview on page 45

IPv4 and IPv6 operation overview

- If IPV6STAT is set to 1, that is, IPv6 is supported, then the DHCPSTAT parameter is selected:
  - If DHCPSTAT is set to 1, that is, use DHCPv4 only, then IPv4 only is enabled.
  - If DHCPSTAT is set to 3, that is, both IPv4 and IPv6 supported, then dual-stack operation is enabled.

If IPv4-only operation is enabled, the system ignores any IPv6 addresses configured as parameter values and uses the next IPv4 address in the list. If the parameter value does not contain any IPv4 address, the system treats the value as null.

The phones in this release support the following combinations or IPv4 and IPv6 IP address configuration:

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

The following table provides the results of the determination:

Table 1: IP Enablement Results

Manually programmed IPv4 address	IPV6STAT	Manually programmed IPv6 address	DHCPSTAT	Result	Addressing modes	
					IPv4	IPv6
No	0	NA	NA	IPv4 only	DHCP	NA
	1	No	1	IPv4 only	DHCP	NA
Yes	0	NA	NA	IPv4 only	Manual	NA
	1	No	1	IPv4 only	Manual	NA

Multi Device Access operation in dual-stack mode

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

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

- LLDP

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

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

Chapter 5: Security configuration

Security overview

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

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

The following security features are available:

- Account management: The phone supports the following:
  - Storage of passwords and user credentials using Federal Information Processing Standards (FIPS 140–2)
  - FIPS 140-2 cryptographic algorithms for application, processes, and users
  - Control to toggle between FIPS and non-FIPS modes
  - Identity certificate installation using Simple Certificate Enrollment Protocol (SCEP) for enrollment and encrypted PKCS#12 file format to import both private key and certificate.
- Certificate management: The phone supports the following:
  - X509v3 compliant certificates
  - Public Key Infrastructure (PKI) for users who use third-party certificates for all Avaya services including database
  - Online Certificate Status Protocol (OCSP) for obtaining the revocation status of an X.509 digital certificate according to RFC 6960
- Department of Defense solution deployment with Joint Inter-operability Test Command (JITC) compliance.
- VLAN separation mode using system parameters.
- Synchronization of the system clock at configured intervals using system parameters.
- Display of SSH fingerprint in the Administration menu.
- Display of SSH fingerprint in the Administration menu.
- Display of OpenSSH and OpenSSL version in the Administration menu.
- Display of OpenSSH and OpenSSL version in the Administration menu.

- Maintenance of integrity when the phone is under Denial of Service (DoS) attack. In this case, the phone goes into out-of-service mode.
- DRBG random number generator compliant with SSL FIPS 140–2.
- SHA2 hash algorithm and strong encryption (256 bit symmetric and RSA 2048 and 4096 bit asymmetric keys) for all cryptographic operations.
- Deprecated support for SHA1 algorithms in all cryptographic algorithms.
- SRTP/SRTCP and TLS v1.2.

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

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

Note:

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

Device lock management parameters

Parameter name	Default value	Description
ENABLE_PHONE_LOCK	0	Specifies whether the **Lock** softkey and lock feature button are enabled on the phone. If you enable the parameter, then a user can lock the phone by pressing the button or selecting the feature. The options are: • 0: Disabled • 1: Enabled

Table continues…

Parameter name	Default value	Description
PHONE_LOCK_IDLETIME	0	Specifies the interval of idle time, in minutes, after which the phone will automatically get locked. Valid values are from 0 to 10080. The options are: • 0: Phone will not lock automatically • 1: Phone will lock automatically

User and account management parameters

Phones support the following parameters for managing the Administration menu for local procedures:

Parameter name	Default value	Description
PROCSTAT	0	Specifies whether local or CRAFT procedures can be used to configure the phone. The options are: • 0: Local procedures can be used • 1: Local procedures cannot be used
PROCPSWD	27238	Specifies an authentication code to access Administration menu. The options are: • 27238: Specifies that the authentication code `27238` is set for accessing local or craft administration procedures • ASCII numbers between 0–7: Specifies an administrator—configured authentication code. You must provide at least four ASCII numbers. • Null: Specifies that no authentication code is required to access the local or craft procedures.
ADMIN_PASSWORD	27238	Specifies an authentication code for accessing the local (craft) procedures screen. This parameter can be set in System Manager and File Server. When the parameter ADMIN_PASSWORD is not set, then the parameter PROCPSWD is used. PROCPSWD supports only numeric values. ADMIN_PASSWORD supports both

Table continues…

Parameter name	Default value	Description
		alphanumeric and special characters. Hence, for enhanced security, use ADMIN_PASSWORD instead of PROCPSWD. You must provide an authentication code for ADMIN_PASSWORD by using a combination of: • Numbers (0–9) • Alphabets in uppercase (A-Z) • Alphabets in lowercase (a-z) • Special characters, except the double quote character (")
ADMIN_LOGIN_ATTEMPT_ALLOWED	10	Specifies the number of failed attempts allowed for accessing the Administration menu for a duration as specified in the parameter. Valid values are between 1 to 20.
ADMIN_LOGIN_LOCKED_TIME	10 minutes	Specifies the duration of lockout when a user reaches the maximum attempts limit to access the Administration menu. Valid values are between 5 to 1440 minutes.

Access control and security

Phones provide the following security features for control and access:

Security event logging

Logs are maintained for the following events:

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

Private Key storage

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

Temporary Data

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

IP information

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

The parameter PROVIDE_NETWORKINFO_SCREEN controls the display of this information.

OpenSSH/OpenSSL version

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

SSH Fingerprint

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

Time synchronization

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

- Default: 1440 minutes
- 60–2880 minutes

Certificate management

Certificates are used to establish secure communication between network entities. Server or mutual authentication can be used to establish a secure connection between a client and server. The client always validates the certificate of the server and maintains a trust store to support this validation. If the server additionally requires mutual authentication, it requests an identity certificate from the client. The identity certificate must be provided and validated by the server to establish mutual authentication. Server must validate the identity certificate to establish a secure connection..

Phones support three types of certificates:

- Trusted certificates
- Online Certificate Status Protocol (OCSP) trust certificates
- Phone identity certificates

The Trusted and OCSP trust certificates are root or intermediate Certification Authority (CA) certificates that are installed on the phone through the `46xxsettings.txt` file.

Enhancements for installing identity certificates:

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

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

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

Trusted certificates

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

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

OCSP trust certificates

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

OCSP Trust Certificates are installed in the same way as those for System Manager. However, OCSP Trust Certificates use a different parameter name called OCSP_TRUSTCERTS. This parameter follows the same format as that for TRUSTCERTS.

Phone identity certificates

Identity certificates are used to establish the identity of a client or server during a TLS session. Phones support the installation of an identity certificate using one of the following methods:

- Secure Certificate Enrollment Protocol (SCEP) by using the `46xxsettings.txt` file parameter MYCERTURL.

  ```
  SET MYCERTURL "http://192.168.0.1/ejbca/publicweb/apply/scep/pkiclient.exe"
  ```

- PKCS12 File by using the `46xxsettings.txt` file parameter PKCS12URL

  ```
  SET PKCS12URL http://192.168.0.1/client_$MACADDR_cert.p12
  ```

Note:

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

The attributes of an identity certificate can be viewed by using a MIB browser. The following MIB OIDs can be used for this query:

Attribute Name	MIB OID
Serial Number	endptIdentityCertSN

Table continues…

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

Server certificate validation

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

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

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

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

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

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

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

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

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

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

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

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

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

Note:

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

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

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

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

Note:

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

FIPS mode

The Federal Information Processing Standard, or FIPS 140-2, is a computer security standard used by the U.S. government to approve cryptographic modules. OpenSSL libraries include a set of cryptographic algorithms compliant with FIPS 140-2, which can be invoked when the library is initiated in FIPS mode. The parameter FIPS_ENABLED controls the usage of OpenSSL FIPS certified cryptographic modules. You can set the parameter through the `46xxsettings.txt` file or DHCP option 242. The description of the parameter is as follows:

Parameter name	Default value	Description
FIPS_ENABLED	0	Specifies whether only FIPS-approved cryptographic algorithms will be supported. The options are: • 0: No restriction on using cryptographic algorithms that are not FIPS-approved. • 1: Use only FIPS-approved cryptographic algorithms using embedded FIPS 140-2 validated cryptographic module.

Ensure that the value of the parameter CONFIG_SERVER_SECURE_MODE is set to 1 when the phone is in FIPS mode.

When you enable FIPS mode, you must disable the following features on the phone:

- SSH Server.
- SCEP certificate enrollment: When a phone runs in FIPS mode, identity certificate enrollment through SCEP is disabled by the software. If identity certificate is generated before FIPS_ENABLED is set to 1, it can still use the existing identity certificate after phone reboot. However, you must not use identity certificates generated using SCEP when FIPS_ENABLED is set to 0 when the phone is configured to work in FIPS mode. The most secure way to install identity certificate is to clear any installed identity certificate and install PKCS#12 file after configuring the phone to FIPS mode. Thereafter, FIPS 140-2 approved cryptographic algorithms can be used to decrypt PKCS#12 file.
- SLA Mon.
- 802.1x with EAP-MD5 or EAP-PEAP authentication. EAP-TLS is allowed.
- WML Browser.
- Push.
- HTTPSRVR. You must use TLSSRVR for file downloading.
- HTTP in OCSP_URI or Authority Information Access (AIA) of a certificate. Ensure that the URI in OCSP_URI or AIA of a certificate is HTTPS.
- Microsoft™ Exchange

When you enable FIPS mode, the phone reboots and runs the OpenSSL FIPS self-test. When the test is completed successfully, the phone displays the message `FIPS mode activated, restarting`…. After reboot, FIPS mode is in effect. If the FIPS-mode self-test fails, the phone displays the message `FIPS self-test failure`. In this case, the phone also displays two options:

- **Program**: The phone prompts for a CRAFT password. After you enter the CRAFT password, the phone boots up in non-FIPS mode.
- **Reboot**: The phone reboots.

Note:

All the logs are stored in SYSLOG. These logs might be referred to for the troubleshooting purpose.

Chapter 6: Phone administration

Introduction

During installation or after you have successfully installed a Avaya J169/J179 IP Phone , you might be instructed to administer one of the manual procedures described in this chapter. These local administrative procedures are also referred to as Craft Procedures.

Note:

You can modify the settings file to set parameters for the phones that download their upgrade script and application files from the same HTTP server. Only trained installers or technicians must perform local (craft) procedures. Perform these procedures only if instructed to do so by the system or LAN administrator.

Static administration of these options causes upgrades to work differently than if they are administered dynamically. Values assigned to options in static administration are not changed by upgrade scripts. These values remain stored in the phone until you use the local administrative procedures RESET.

Use these option-setting procedures only with static addressing and, as always, only if instructed by the system or LAN administrator. Do not use these option-setting procedures if you are using DHCP.

About local administrative procedures

Craft procedures allow you to customize the IP phone installation for your specific operating environment. This section provides a description of each local administrative option covered in this guide.

Note:

By default, a user can view but not change most of the parameters associated with Craft procedures.

Options	Purpose
802.1X	Specifies the 802.1X operational mode.
ADDR	Specifies the network address information.
AGC	Enables or disables Automatic Gain Control.

Table continues…

Options	Purpose
CALIBRATION	Calibrates the touchscreen (9621G and 9641G models only).
RESET	Resets all values to factory defaults.
DEBUG	Enables or disables Debug Mode.
GROUP	Sets the Group Identifier.
HANDSET EQ	Sets the handset equalization.
INT	Specifies the network interface control.
LOG	Enables or disables the event logging.
LOGOUT	Logs off the phone.
RESET VALUES	Resets system initialization values to default.
RESTART PHONE	Restarts the phone.
SIG	Sets the signaling protocol download flag.
SIP	Configures the SIP call settings.
SNTP	Configures the time server settings.
SSON	Sets the Site-Specific Option Number.
VIEW	Shows current parameter values and file names.

Accessing the Administration menu

The Local or the CRAFT procedures can only be invoked if the value of the PROCSTAT parameter in the `46xxsettings.txt` file is set to **0**. Setting the PROCSTAT parameter to **0** provides full access to the local procedures. You can access the Administration menu during phone startup and during normal phone operation.

Note:

You cannot answer a call when the phone displays the Administration password screen.

For all non-touchscreen phones, use the navigation arrows to scroll to and highlight the local procedure you want, then press **Select** or **OK**. Or scroll to the procedure you want and press the corresponding line button. For touchscreen phones, scroll to the local procedure you want if it not already displayed then touch the line on which the local procedure you want appears.

Accessing the Administration menu during phone startup

About this task

You can access the Administration menu during phone startup using the following steps.

Before you begin

The default password to gain access to the local procedures menu is set in PROCPSWD or ADMIN_PASSWORD parameter. The factory-set default password is **27238**. You must not change the default value at the time of initial installation.

Procedure

1. Press **Admin** .
2. Enter the administrator password.
3. Press the **Enter** softkey.

Accessing the Administration menu after phone startup

Procedure

1. Press **Avaya Menu** for button phones or **Avaya Home** for touchscreen phones.
    - For touchscreen phones, tap **Settings** icon.
    - For button phones, scroll down to **Administration** option.
2. Do one of the following:
    - For touchscreen phones, scroll down and tap **Administration**.
    - For button phones, press **Select**.
3. Enter the administrator password on the Enter access code screen.
4. Select **Enter**.

Administering the phone by using local procedures

This section explains how to use the local administrative procedures on the phone UI for administration. The local procedures that you can administer on the phone are:

- 802.1X - To set the 802.1X operational mode.
- ADDR - To set the static addresses.
- AGC - To enable or disable Automatic Gain Control.
- RESET - To reset all administered values, user-specified data, option settings, etc. and return the phone to its initial "out of the box" default values.
- DEBUG - To enable or disable debug mode for the button module serial port.
- GROUP - To set the group identifier on a per-deskphone basis.
- HANDSET EQ - To set the handset equalization settings of the deskphone.
- INT - To locally enable or disable the secondary Ethernet hub.

- LOG - To enable or disable event logging.
- LOGOUT - To logout the user from the deskphone.
- RESET VALUES - To reset the deskphone to default values including the registration extension and password, any values administered through local procedures, and values previously downloaded using DHCP or a settings file.
- RESTART PHONE - To restart the deskphone in response to an error condition, including the option to reset parameter values.
- SIG **-** To change the default signaling value from SIP to H.323 or vice versa.
- SIP - To configure SIP call settings.

⚠ **Warning:**

The SIP call settings entered through the Administration menu take precedence over other sources for this data, for example- `46xxsettings.txt` file, or PPM. The only way to override these settings is to go into the Administration menu and remove the settings or perform a RESET of the phone from the Administration menu.

- SNTP - To configure the time server settings.
- SSON - To set the site-specific option number.
- VIEW - To review the system parameters for the deskphone to verify current values and file versions.

Applications and features provisioning

You can configure the following parameters to enable or disable certain applications and general phone features. The following table lists the features and applications and their corresponding parameters that enable

Application or feature	Parameter name	Description
History application	ENABLE_CALL_LOG	If enabled, users can access the list of unanswered and answered calls. If disabled, the History application is not displayed to the user and calls are not logged.
Redial	ENABLE_REDIAL	If enabled, users can redial one to three previously called numbers. If disabled, redialing is not available to the end user.
Redial list	ENABLE_REDIAL_LIST	If enabled, users can select a number to redial from a list. If disabled, only the previously-dialed number can be redialed.
Contacts application	ENABLE_CONTACTS	If enabled, users can access a list of numbers and make calls by selecting a contact name or number. If disabled, the deskphone does not display the Contacts application and users cannot set up or maintain the contact list.

Table continues…

Application or feature	Parameter name	Description
Contacts modification	ENABLE_MODIFY_CONTACTS	If enabled, users can change or update the contact list. If disabled, users cannot change or update the contact list.
Exchange contacts	PROVIDE_EXCHANGE_CONTACTS	If enabled, users can gain access to contacts stored in the Exchange server through the Contact list, by pressing the Exchange contact button. If disabled, users cannot gain access to the Exchange contacts.
Options & Settings menu option	PROVIDE_OPTIONS_SCREEN	If enabled, the deskphone displays the Options & Settings menu option in the Avaya menu or Home Screen. If disabled, the deskphone does not display the Options & Settings menu option. Users cannot change any of the features and ppeonfiasscnted with the Options & Settings menu.
Network Information menu option	PROVIDE_NETWORKINFO_SCREEN	If enabled, the deskphone displays the Network Information menu option in the Avaya menu or Home Screen. If disabled, the deskphone does not display the Network Information menu option.
Logout menu option	PROVIDE_LOGOUT	If enabled, the deskphone displays the Logout menu option in the Avaya menu or Home Screen. If disabled, the deskphone does not display the Logout menu option.
Exchange calendar	PROVIDE_EXCHANGE_CALENDAR	If enabled, users can integrate and gain access to the Exchange calendar on the deskphone. If disabled, users cannot gain access to the Exchange calendar on the deskphone.

Chapter 7: Failover and survivability

Redundancy with IP phone and Avaya Aura®

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

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

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

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

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

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

Detection of loss of connection

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

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

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

Failover to a backup proxy

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

Restoring the phone to the primary proxy

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

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

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

Proxy determination when the connection to the primary proxy is lost

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

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

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

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

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

Simultaneous registration

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

Note:

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

Limitations during failover or failback

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

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

Preserved call

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

Limitations of a preserved call

In a successful call preservation, the audio path is preserved. However, in a preserved call, the phone does not support call features, for example, conference call, call transfer, and call forward . The reason is loss of signaling between the phone and the SIP proxy that was used when the call was initially established.

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

- If one of the calling parties disconnects from a preserved call, the other end might not be disconnected.
- Communication Manager cannot perform mid-call operations, such as MLPP features, when the target phone is in a connection preserved state.

Supported non Avaya Aura® proxies for redundancy

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

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

Limitations after a successful failover

Failover to a Session Manager

instance

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

Failover to a Branch Session Manager

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

Note:

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

Failover to a proxy other than Avaya Aura®

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

- A conference is limited to three parties and is hosted by the phone.
- Contacts can be used and new contacts can be saved on the phone. New contacts are cached on the phone, and after failback to Avaya Aura®, the new contacts are synchronized with Avaya Aura®.
- The dial plan for Avaya Aura® is unavailable. Instead, the dial plan configured in the `46xxsettings.txt` file is used.
- The following Avaya Aura® features are unavailable:
    - Last party drop
    - Send All Calls (Do Not Disturb)
    - Presence
    - Calling party block/unblock
    - Call park/unpark
    - All forms of call pickup

- Priority calls
- MLPP functionality
- Auto callback
- Malicious call trace
- EC500 on/off
- Transfer to voicemail
- Paging
- Call recording
- Bridge Line Appearance
- Extend call
- Hold recall
- Transfer recall
- Busy Indicator
- Message Waiting Indicator
- Team button
- Call Center Elite

Indications of redundancy

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

Acquiring service

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

⚠

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

Preserved call

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

⚠

Parameters for redundancy provisioning

SIP connection parameters

Parameter name	Default value	Description	System Manager parameter name
CONTROLLER_SEARCH_INTERVAL	16	Specifies the number of seconds the phone will wait to complete the maintenance check for monitored controllers. Valid values are from 4 to 3600.	NA
DISCOVER_AVAYA_ENVIRONMENT	1	Specifies dynamic feature set discovery. Value operation are: • 0: Non-Avaya environment. Does not auto-discover Avaya SIP Telephony (AST) support . • 1: Avaya environment. Auto-discovers AST support. The SIP proxy server or controller might not support AST.	NA
FAILBACK_POLICY		Specifies the policy in effect for recovery from failover. Value operation: • Admin: The phone waits for administrative intervention before failing back to a higher priority controller. • Auto: The phone periodically checks the availability of the primary controller and fails back to the primary controller if available.	Failback Policy The value set in System Manager overwrites the value in the `46xxsettings.txt` file.
FAST_RESPONSE_TIMEOUT	4	Specifies the number of seconds the phone will wait before terminating an invite transaction if no response is received. Valid values are from 0 to 32. Value operation: • 0: Timer is disabled	Timer B This parameter is mandatory in System Manager and the default value is 2 seconds. The value set in System Manager overwrites the value in the `46xxsettings.txt` file.

Table continues…

Parameter name	Default value	Description	System Manager parameter name
RECOVERYREGISTERWAIT	60	Specifies the number of seconds. If no response is received by WAIT_FOR_REGISTRATION_TIMER to a REGISTER request within the specified number of seconds, the phone tries again after a randomly selected delay of 50% to 90% of the value of RECOVERYREGISTERWAIT. Valid values are from 10 to 36000.	Reactive Monitoring
REGISTERWAIT	900	Specifies the number of seconds for next re-registration to the SIP proxy. Valid values are from 30 to 86400 seconds.	Registration Expiry Timer The value set in System Manager overwrites the value in the`46xxsettings.txt` file.
WAIT_FOR_REGISTRATION_TIMER	32	Specifies the number of seconds the phone will wait for a response to a REGISTER request. If no response message is received within this time, the phone tries to register again based on the value of RECOVERYREGISTERWAIT. Valid values are from 4 to 3600.	NA
SIP_CONTROLLER_LIST	Null	Specifies a list of SIP controller designators, separated by commas without any intervening spaces. When this parameter has multiple IP addresses, the list order defines the priority of the controllers for selection during a failover. The first element of the list has the highest priority, and the last element has the lowest priority.	Primary Session Manager, Secondary Session Manager and Survivability server
ENABLE_PPM_SOURCED_SIPPROXYSRVR	1	Enables PPM as a source of SIP proxy server information.	NA

Table continues…

Parameter name	Default value	Description	System Manager parameter name
		Value operation: • 0: Proxy server information received from PPM is not used. • 1: Proxy server information received from PPM is used.	
SIP_CONTROLLER_LIST_2	Null	Replaces SIP_CONTROLLER_LIST for IPv4 and IPv6 phones. It is used to select the registration address.	Primary Session Manager, Secondary Session Manager, and Survivability server.
SIMULTANEOUS_REGISTRATIONS	3	Specifies the number of simultaneous Session Manager and Branch Session Manager registrations that the phone must maintain. Valid values are from 1 to 3. The value of this parameter must not be less than the number of core Session Manager instances in SIP_CONTROLLER_LIST.	NA
SIPREGPROXYPOLICY	alternate	Specifies whether the telephone will attempt to maintain one or multiple simultaneous registrations. Value operation: • Alternate: The phone registers only to the first controller in the list. If the phone cannot reach the first controller, the phone registers to the second controller . • Simultaneous: The phone simultaneously registers to more than one SIP proxy controller at the same time.	NA

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

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

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

Table continues…

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

Redundancy in a non-Avaya proxy environment

In an Avaya environment, the SIP proxy list is defined using dotted decimal notation to define the proxy addresses. In a non-Avaya environment, where FQDNs are used to define the SIP proxy, there can only be one proxy. In this case, redundancy is not supported.

Chapter 8: Backup and restore

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.

Table continues…

Parameter	Default value	Description
ENABLE_PHONE_LOCK	0	Specifies whether the **Lock** softkey and the Lock feature button are displayed on the phone.
SHOW_CALL_APPEARANCE_NUMBERS	0	Specifies whether for a user the device displays call appearance numbers in the call containers.

Chapter 9: Phone upgrade

Upgrading the device

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 ways:

- Automatic: You can configure the device to poll periodically for a newer version of the software in the file server and automatically download the software and upgrade itself.
- Manual: You can upgrade the device without the device waiting for a polling interval manually.

Related links

Downloading and saving the software on page 32

Downloading and saving the software

Before you begin

Ensure that your file server is set up.

Procedure

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

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

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

   The system displays the Downloads page.

9. In the **File** field, click the settings file and save the file at an appropriate location on the file server.

Related links

File Server configuration on page 28
Upgrading the device on page 83

Upgrading the device manually

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.

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.

Downloading text language files

Language files contain the language name (as it should be presented to a user for selection), an indication of the preferred character input method, text string replacements for the built-in English text strings, where each replacement string may contain up to 120 characters. Each has a unique index that associates it with the corresponding built-in English string, an indication as to whether Chinese, Japanese or Korean glyphs should be displayed for the Unicode "Unified Han" character codes, and a Language Identification Tag for the language of the text contained in the file. A downloadable language file may also contain a translation of the language name into any or all of the languages for which a language file is included in the software distribution package. Language files must be stored in the same location as the 46xxsettings.txt file.

You can download a new language file version only if the filename differs from the language file previously downloaded. Alternately, you can remove the old language file using an empty **SET LANGUAGES** command in the 46xxsettings file before downloading a language file with the same filename.

Note:

Changing the signaling protocol

About this task

For enterprises requiring both H.323-based and SIP-based protocols, there are two ways to specify the protocol to be used by all or specific phones:

Procedure

1. The SIG parameter can be set in DHCP Option 242 (Site-Specific Option Number) or in the `46xxsettings.txt` file. This setting will apply to all phones except those for which SIG has been manually configured to a value of H.323 or SIP using the SIG Craft procedure.
2. The SIG parameter can be set on each phone.

The GROUP parameter

You might have different communities of end users, all of which have the same model deskphone, but which require different administered settings. For example, you might want to restrict Call Center agents from being able to log off, which might be an essential capability for "hot-desking" associates. We provide examples of the group settings for each of these situations later in this section.

The simplest way to separate groups of users is to associate each of them with a number. Use the GROUP system value for this purpose. The GROUP system value **cannot** be set in the 46xxsettings file. The GROUP system value can only be set on each deskphone using a Craft procedure. To set up groups, first identify which deskphones are associated with which group and designate a number for each group. The number can be any integer from 0 to 999, with 0 as the default, meaning your largest group would be assigned as Group 0.

Then, at each non-default deskphone, invoke the **GROUP** Local (Craft) Administrative procedure and specify which GROUP number to use. Once the GROUP assignments are in place, edit the configuration file to allow each deskphone of the appropriate group to download its proper settings.

Here is an illustration of a possible settings file for the example of a Call Center with hot-desking associates at the same location:

```
IF $GROUP SEQ 1 goto GROUP1 IF $GROUP SEQ 2 goto GROUP2 {specify settings unique to
Group 0} goto END # GROUP1 {specify settings unique to Group 1} goto END # GROUP2
{specify settings unique to Group 2} # END {specify settings common to all Groups
```

Chapter 10: Troubleshooting

Error conditions

There are three areas where installers can troubleshoot problems before seeking assistance from the system or LAN administrator:

- Check both the power and Ethernet wiring for the following conditions:
    - Whether all components are plugged in correctly.
    - Check LAN connectivity in both directions to all servers - DHCP, HTTP, HTTPS, Avaya Communication Manager, and/or SIP Proxy server.
    - If the phone is supposed to be powered from the LAN, ensure that the LAN is properly administered and is compliant with IEEE 803.3af.
- If you are using static addressing:
    - Use the **VIEW** Craft procedure to find the names of the files being used and verify that these filenames match those on the HTTP/HTTPS server.
    - Use the **ADDR** Craft procedure to verify IP Addresses.
- If the phones are not communicating with the system (DHCP, HTTP, or Communication Manager call server), make a note of the last message displayed. Consult the system administrator.
- If you expect the phone to be IEEE-powered, verify with the LAN administrator that IEEE power is indeed supported on the LAN.

Related links

DTMF tones on page 87

Power interruption on page 88

DTMF tones

SIP deskphones send DTMF tones according to the SEND_DTMF_TYPE parameter setting. The default setting of this parameter sends DTMF "tones" as "telephone event" RTP packets per RFC 2833. Whether a non-SIP deskphone hears these DTMF tones depends on whether the Avaya Communication Manager media resource converts the "telephone event" RTP packets into audio RTP packets.

Related links

Error conditions on page 87

Power interruption

If power to the phone is interrupted while the phone is saving the application file, the HTTP/HTTPS application can stop responding. If this occurs, restart the phone.

Related links

Error conditions on page 87

Installation error and status messages

The Avaya J100 Series IP Phones issue messages in the currently selected language, or if the phone is logged off, in the language specified by the SYSTEM_LANGUAGE parameter value. If English is not the selected language, the phone displays messages in English only when they are associated with local procedures, for example, the **VIEW** Craft local procedure.

Most of the messages described in the table appears only for about 30 seconds or less, and then the phone resets. The most common exception is

`Extension in Use`

, which requires manual intervention.

Possible error and status messages during installation of the phones

Message	Cause/Resolution
`Address Conflict`	Cause: The phone has detected an IP Address conflict. Resolution: Verify administration to identify duplicate IP Address(es).
`Bad Router`	Cause: The phone cannot find a router based on the information in the DHCP file. Resolution: Use static addressing to specify a router address, or change administration on DHCP.
`DHCP: CONFLICT`	Cause: At least one of the IP Addresses offered by the DHCP server conflicts with another address. Resolution: Review DHCP server administration to identify duplicate IP Address(es).
`Finding router...`	Cause: The phone is proceeding through boot-up. Resolution: Allow the phone to continue.
`No Ethernet`	Cause: When first plugged in (or during operation), the SIP IP phone is unable to communicate with the Ethernet.

Table continues…

Message	Cause/Resolution
	Resolution: Verify the connection to the Ethernet jack, verify the jack is Category 5, verify power is applied on the LAN to that jack, etc.
`Restarting...`	Cause: The phone is in the initial stage of rebooting. Resolution: Allow the phone to continue.
`SCEP: Failed`	Cause: Simple Certificate Enrollment Protocol (SCEP) has rejected a request for a certificate. Resolution: Although the SCEP server connection is terminated, startup continues. No action required.
`Subnet conflict`	Cause: The phone is not on the same VLAN subnet as the router. Resolution: Administer an IP Address on the phone using static address or or administer network equipment to administer the phone appropriately.
`Updating: DO NOT UNPLUG THE TELEPHONE`	Cause: The phone is updating its software image. Resolution: Allow the phone to continue.

Operational errors and status messages

The table described identifies some of the possible operational problems that might be encountered after successful installation of the phone. The user guide for a specific phone model also contains troubleshooting for users having problems with specific phone applications.

Possible operational error conditions

Condition	Cause/Resolution	
During Craft procedure access, display freezes at prompt "Press * to program"	Cause: Craft access has failed; phone cannot operate. Resolution: Unplug the phone, then plug it in again to reset.	
After Login, the progress bar shows just a few completed bars and stops moving.	Cause: Login has failed. Resolution: Check that the LAN and File servers are operating correctly. Re-attempt login.	
The message light on the phone turns on and off intermittently, but the phone never registers.	Cause: This is a hardware fault. Resolution: The phone must be returned to Avaya for repair.	
The phone stops working in the middle of a call.	No lights are lit on the phone and the display is not lit.	Cause: Loss of power. Resolution: Check the connections between the phone,

Table continues…

		the power supply, and the power jack.
	Phone might have gone through the restarting sequence.	Cause: Loss of path to the call server or the other party's phone, DHCP Lease expired, or DHCP server not available when phone attempts to renegotiate DHCP lease. Resolution: Check the connections between the phone, the power supply, and the power jack.
The phone was working, but does not work now.	No lights are lit on the phone and the display is not lit.	Cause: Loss of power. Resolution: Check the connections between the phone, the power supply, and the power jack.
	Power to the phone is fine, but there is no dial tone or the call appearances or feature buttons do not work.	Cause: Loss of communication with the call server. Resolution: Check LAN continuity from the call server to the phone using ARP or trace-route and from the phone to the call server by invoking a Feature button. Verify that administration has not changed for the LAN equipment (routers, servers, etc.) between the call server and the phone. Verify no one changed the phone settings locally using the **View** and **ADDR** craft procedures, as described earlier in this guide.
	The phone was recently moved.	Cause: Loss of communication with the call server. Resolution: As above, but pay particular attention to the possibility that the phone is being routed to a different DHCP server, or even a different proxy server. If so, the new server might need to be administered to support the phone.
	The network was recently changed to upgrade or replace servers, re-administer the	Cause: Loss of communication with Session Manager. Resolution: As above.

Table continues…

	Communication Manager call server, add or change NAT, etc.	
The phone works, but the audio quality is poor.	The user hears echo when speaking on a handset.	Cause: Echo from digital-to-analog conversion on your Communication Manager call server trunk. Resolution 1: Try a different Call Quality setting under the Audio Parameters section. Resolution 2: Check whether packet loss, or jitter delay is causing this problem, by eliminating or minimizing both. Resolution 3: Verify which trunk is causing the echo, and check the trunk's Trunk Termination parameter on the call server.
	The user hears echo on a headset, but not on a handset.	Cause: Improper headset adapter. Resolution: Replace adapter with Avaya's M12LU or 3412-HIC adapters. We recommend the M12LU, since it supports Automatic Gain Control.
	The user is on Speaker and hears no echo, but the far-end hears echo.	Cause: Room acoustics. Resolution: Ensure that there are six inches or so of blank space to the right of the phone. If that is insufficient, use the handset.
	the user experiences sudden silences such as gaps in speech, or static, clipped or garbled speech, etc.	Cause: Jitter, delay, dropped packets, etc. Resolution: You can have the user provide diagnostic data by invoking the Network Information feature under the **A** (Avaya) button on the phone. One or more Quality of Service (QoS) features should be implemented in the network. Cause: Improper non-Category 5 wiring. Resolution: Replace non-Category 5 wiring with Category 5 wiring.

Table continues…

	The user hears fluctuations in the volume level which are worse when the Speaker is on, or at the beginning of a call, or when a call goes from no one talking abruptly to a loud voice.	Cause: The user has changed the Automatic Gain Control (AGC) or environmental acoustics are not consistent with the current audio settings. Resolution: Try different on/off settings for the AGCHAND, AGCHEAD, and AGCSPKR parameters.
The phone works properly except for the Speaker.	Cause: The Speaker was disabled in the settings file. Resolution: Check the settings file and re-enable the Speaker if appropriate.	
The phone works properly, except incoming DTMF tones are not received.	Cause: The TN2302AP board does not pass in-band DTMF tones. Resolution: None; the board is operating as designed.	
When a line is selected, a short dial tone burst sounds followed by a reorder/fast busy tone.	Cause: The extension is provisioned on Session Manager and some Communication Manager forms, but not on the off-pbx-telephone station-mapping form. Communication Manager is unable to map back to Session Manager, and rejects the line reservation. Resolution: Map the extension on the off-pbx-telephone station-mapping form. Cause: Possible error in SIG group configuration on Communication Manager, which indicates the default region for the SIP trunk to Communication Manager. Resolution: On the IP-network-region form, ensure that the region pointed to is configured with an **authoritative domain** that is the same as the Session Manager SIP domain. also verify that the station in question has not been redirected to a different network region on the ip-network map.	
The HTTP/HTTPS script file and settings file are ignored (not being used by the phone).	Cause: The system value AUTH is set to 1 (HTTPS required) but no valid address is specified in TLSSRVR. Resolution: Change AUTH to 0 (zero), or enter a valid address for TLSSRVR.	
The HTTP/HTTPS script file is ignored or not used by the phone.	The HTTP/ HTTPS server is a LINUX or UNIX system.	Cause: UNIX and LINUX systems use case-sensitive addressing and file labels. Resolution: Verify the file names and path in the script file are accurately specified.
	The phone administration recently changed.	Cause: The ***J100Supgrade.txt*** file was edited incorrectly, renamed, etc.

Table continues…

		Resolution: Download a clean copy of the ***J100Supgrade.txt*** file from the Avaya support siteand do not edit or rename it. Customize or change only the ***46xxsettings*** file.
The MS Exchange contacts take too long to load	Cause: The correct Exchange server is not specified in the parameter EXCHANGE_SERVER_LIST in the ***46xxsettings*** file. Resolution: Verify that the MS Exchange server being used is specified in the settings file. To view the Exchange server in use, go to: **Outlook** > **Tools>Options** > **Mail Setup** > **E-mail Accounts** > **Change** .	
Some settings in the settings file are being ignored while other settings are being used properly.	Cause: Improper settings file administration. Resolution: Verify that customized settings are correctly spelled and formatted.	
	The setting being ignored is one or more of the AGC settings.	Cause: The user changed the AGC setting(s). Resolution: Have the user reset the AGC value(s) back to the desired setting(s).
	The setting being ignored is the TIMEFORMAT setting.	Cause: The time format was changed using the Avaya Menu Options & Settings. Resolution: If the time disappears, Reboot the phone.
Phone power is interrupted while the phone is saving the application file and the HTTP/ HTTPS application stops responding.	Cause: The HTTP/HTTPS application stops responding if power is interrupted while a phone is saving the application file. Resolution: Restart the phone.	
The user indicates an application or option is not available.	Cause: The ***46xxsettings*** script file is not pointed to accurately, or is not properly administered to allow the application. Resolution: Assuming the user is meant to have that application, verify the 46xxsettings script file is properly specified for your system, including case if your file server is UNIX or LINUX, and extension. Then, verify all the relevant parameters.	
User data disappeared when the user logged off one phone and logged into another phone.	Cause: Possible PPM problem. Resolution: Contact the Session Manager administrator.	
The phone displays "User logged in at another location".	Cause: The extension entered by the user during login is currently in use on another phone. Resolution: Instruct user to log in with a different extension. Tell the user to press the 'Retry' softkey, then enter new extension and	

Table continues…

	password. Or, have the user log in with the original extension, while unregistered the extension from the other phone.
Login fails	Cause: Invalid provisioning on Communication Manager or Session Manager. Resolution: Session Manager needs to point to Communication Manager's PROCR interface for the "Media Server Admin Address." Session Manager must point to a specially-provisioned PPM Administration account on Communication Manager. The PPM Administration account on the Communication Manager side must have several specific parameters set. Specifically: login group must be "susers" additional group must be "prof18" or equivalent shell access must be "no shell access".
Multiple call appearances on incoming call.	Cause: Provisioning problem. Resolution: On the off-pbx-telephone station-mapping form, set the Bridged Calls field to "none".
A blank screensaver appears and the phone does not immediately respond to pressing the Phone button	Cause: The server IP Address in the LOGO parameter is invalid or unavailable. Resolution: Correct/change the LOGO parameter in the settings file.

SRTP provisioning

SRTP is now supported (with TLS). To use SRTP, the network region codec set must have media encryption set up for each region that calls may traverse.

When SRTP is provisioned in Communication Manager, the default cryptosuite used is ‘aescm128-hmac80’. The phone also assumes that no encryption is an option provisioned in Communication Manager. If Communication Manager is provisioned with the cryptosuite aescm128-hmac80, then the following entry must be in the 46xxsettings.txt file:

SET MEDIAENCRYPTION "1,9"

If some other encryption set is required, the string must be set appropriately in the 46xxsettings.txt file.

Chapter 11: Appendix

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.
ADMIN_LOGIN_ATTEMPT_ALLOWED	10	Specifies the allowed number of failed attempts to enter the access code before the local or craft procedures gets locked. Valid values are from 1 to 20.
ADMIN_LOGIN_LOCKED_TIME	10	Specifies the duration for lockout when a user reaches the maximum attempts limit for accessing the Administration menu. Valid values are from 5 min. to 1440 min.
ADMIN_PASSWORD	27238	Specifies an access code for accessing the Admin menu. Valid values are from 6 to 31 alphanumeric characters including upper case, lower case characters and special characters. However, double quote character (“) cannot be used for a value of this parameter. ✱ **Note:** • If this parameter length is set below 6 or above 31 alphanumeric characters, then the parameter is treated as not defined. • If this parameter is set in the `46xxsettings.txt` file, then it replaces PROCPSWD parameter. • If you set ADMIN_PASSWORD in the Avaya Aura® System Manager you require

Table continues…

Parameter name	Default value	Description
		at least Avaya Aura® System Manager 7.1.0. • Setting this parameter through PPM is more secure because this file can usually be accessed and read by anyone on the network. Setting the value in this file is intended primarily for configurations with versions of phone or if server software that do not support setting this value from the server.
AGCHAND	1	Specifies the status of Automatic Gain Control (AGC) for the handset. Value Operation: • 0: Disables AGC for the handset. • 1: Enables AGC for the handset.
AGCSPKR	1	Specifies the status of Automatic Gain Control (AGC) for the speaker. Value Operation: • 0: Disables AGC for the speaker. • 1: Enables AGC for the speaker.
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	0	Specifies the level of sidetone in the handset. Value Operation: • 0: Normal level for most users • 1: Three levels softer than normal • 2: Inaudible • 3: One level softer than normal • 4: Two levels softer than normal • 5: Four levels softer than normal • 6: Five levels softer than normal

Table continues…

Parameter name	Default value	Description
		• 7: Six levels softer than normal • 8: One level louder than normal • 9: Two levels louder than normal
AUTH		Specifies whether the script files are downloaded from an authenticated server over an HTTPS link. Value Operation: • 0: Optional • 1: Mandatory
AUTHCTRLSTAT	0	Specifies if the enhanced debugging capabilities can be activated from the SSH server by the Avaya technicians only. Value Operation: • 0: Enhanced debugging capabilities are disabled. • 1: Enhanced debugging capabilities are enabled. The parameter must be set to 1 only for the debugging period by Avaya technicians. Set the 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 • 4: 3db below nominal • 3: 6db below nominal • 2: 9db below nominal • 1:12db below nominal
BRURI	Null	Provides the capability to send a phone report to a server with the URI of the server defined by this parameter. To send the report, go to **Main Menu** > **Admin** > **Debug** > **Phone report**.
C		

Table continues…

Parameter name	Default value	Description
CALL_TRANSFER_MODE	0	Determines the call transfer mode in 3rd party environments. Valid value is 0 or 1.
CALLFWDADDR The parameter is only available in an Avaya Aura® environment.	Null	Sets the address to which calls are forwarded for the call forwarding feature. Users can change or replace this administered value if CALLFWDSTAT is not 0.
CALLFWDDELAY The parameter is only available in an Avaya Aura® environment.		Sets the number of ring cycles before the call is forwarded to the forward or coverage address. The default delay is one ring cycle.
CALLFWDSTAT The parameter is only available in an Avaya Aura® environment.	0	Sets the call forwarding mode of the phone by summing the following values: • 1: Permits unconditional call forwarding. • 2: Permits call forward on busy. • 4: Permits call forward/no answer. • 0: Disables call forwarding. Example: a value of 6 allows call forwarding on busy and on no answer.
CERT_WARNING_DAYS	60	Specifies the number of days before the expiration of a certificate that a warning will first appear on the phone screen. Certificates include trusted certificates, OCSP certificates and identity certificate. Log and syslog message will also be generated. The warning will reappear every seven days.Valid values are from 0 to 99. Value operation: • 0: No certificate expiration warning will be generated.
CERT_WARNING_DAYS_EASG	365	Specifies how many days before the expiration of EASG product certificate that a warning should first appear on the phone screen. Syslog message will be also generated. Valid values are from 90 to 730.
CNGLABEL	1	Determines if personalize button labels can be displayed to the user. Value Operation: • 0: Capability not displayed to the user. • 1: Capability displayed to the user.
CONFERENCE_FACTORY_URI	Null	Specifies the URI for Avaya Aura Conferencing.

Table continues…

Parameter name	Default value	Description
		Valid values contain zero or one URI, where a URI consists of a dial string followed by @, and then the domain name, which must match the routing pattern configured in System Manager for Adhoc Conferencing. Depending on the dial plan, the dial string can need a prefix code, such as a 9 to get an outside line. The domain portion of the URI can be in the form of an IP address or an FQDN. The value can contain 0 to 255 characters. The default value is null.
CONFERENCE_TYPE	1	Determines the selection of the Conference Method. Value Operation: • 0: Local conferencing is supported based on sipping services. • 1: Server based conferencing is supported. • 2: Click-to conference server based conferencing is supported. If the parameter is set to a value that is outside the range then default value is selected. **Note:** The parameter is set to 0 in IP Office environment.
CONFIG_SERVER_SECURE_MODE	1	Specifies whether HTTP or HTTPS is used to access the configuration server. Value Operation: • 0: HTTP • 1: HTTPS • 2: Use HTTPS if SIP transport mode is TLS, otherwise use HTTP. 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 outbound connection to the SIP Proxy and listening socket

Table continues…

Parameter name	Default value	Description
		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	16	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. • 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.

Table continues…

Parameter name	Default value	Description
CURRENT_LOGO	None	Specifies if custom logo or wallpaper is selected for display. The CURRENT_LOGO is used in the following cases: • The phone is not registered to Avaya Aura® Session Manager. • The phone is registered to Avaya Aura® Session Manager and - there is no information stored for the current logo file for this specific user, and - there is no support of Profile Settings in the Endpoint Template. This is supported by Avaya Aura® System Manager 6.3.8 and later. If none is used for logo or wallpaper display, then the phone only displays time or date.
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 (For example, 07). • Use %Y for year with century (For example, 2007). Any character not preceded by % is reproduced exactly.
DAYLIGHT_SAVING_SETTING_MODE		Specifies daylight savings time setting for phone. Value Operation: • 0: Daylight saving time not activated • 1: Daylight saving time is activated. Time set to DSTOFFSET. • 2: Activates automatic daylight savings adjustment as specified by DSTSTART and DSTSTOP.
DELETE_MY_CERT	0	Specifies whether the installed identity certificate, using SCEP or PKCS12 file download, will be deleted. • 0: Installed identity certificate remains valid.

Table continues…

Parameter name	Default value	Description
		• 1: Installed identity certificate is removed.
DHCPSTAT	1	Specifies whether DHCPv4, DHCPv6, or both will be used in case IPv6 support is enable by using IPV6STAT. Value operation: • 1: Run DHCPv4 only. IPv4only-mode, if no own IPv6 address is programmed statically • 2: Run DHCPv6 only. Pv6only-mode, if no own IPv4 address is programmed statically • 3: Run both DHCPv4 & DHCPv6. Dual-stack mode Value 2 or 3 run both DHCPv4 and DHCPv6.
DHCPSTD	0	Specifies whether DHCP complies with the IETF RFC 2131 standard. 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.

Table continues…

Parameter name	Default value	Description
		Note: Set the parameter to 0 for IP Office environment.
DISPLAY_SSL_VERSION	0	Specifies whether OpenSSL and OpenSSH versions are displayed in the **Administration** menu. 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.

Table continues…

Parameter name	Default value	Description
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.
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.
DSTOFFSET	1	Specifies the time offset in hours of daylight savings time from local standard time. Valid values are 0, 1, or 2. The default value is 1.
DSTSTART	2SunMar2L	Specifies when to apply the offset for daylight savings time. The default value is 2SunMar2L (the second Sunday in March at 2AM local time).
DSTSTOP	1SunNov2L	Specifies when to stop applying the offset for daylight savings time. The default value is 1SunNov2L (the first Sunday in November at 2AM local time).
DTMF_PAYLOAD_TYPE	120	Specifies the RTP payload type to be used for RFC 2833 signaling. Valid values are 96 through 127.
E		
EASG_SITE_AUTH_FACTOR	Null	Specifies Site Authentication Factor code associated with the EASG site certificate being installed. Valid values are 10 to 20 character alphanumeric string.
EASG_SITE_CERTS	Null	Specifies list of EASG site certificates which are used by technicians when they don't have access to the Avaya network to generate EASG responses for SSH login. The URLs must be separated by commas without any intervening spaces. Valid values are 0 to 255 ASCII characters.
ELD_SYSNUM	1	Controls whether Enhanced Local Dialing algorithm will be applied for System Numbers-Busy Indicators and Auto Dials.

Table continues…

Parameter name	Default value	Description
		Value operation: • 0: Disable ELD for System Numbers • 1: Enable ELD for System Numbers
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. 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. The phone disables the **Contacts** option on the interface. • 1: Yes **Note:** The parameter is set to 1 in IP Office 10.1 or later. In previous releases it is set to 0.
ENABLE_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.

Table continues…

Parameter name	Default value	Description
		Value Operation: • 0: Disabled • 1: Enabled
ENABLE_G711U	1	Specifies ifr the G.711 mu-law codec is enabled. Value Operation: • 0: Disabled • 1: Enabled
ENABLE_G722	1	Specifies if the G.722 codec is enabled. Value Operation: • 0: Disabled • 1: Enabled
ENABLE_G726	1	Specifies if the G.726 codec is enabled. Value Operation: • 0: Disabled • 1: Enabled
ENABLE_G729	1	Specifies if the G.729A codec is enabled. Value Operation: • 0: Disabled • 1: Enabled without Annex B support (default). • 2: Enabled with Annex B support.
ENABLE_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

Table continues…

Parameter name	Default value	Description
		• 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_OPUS	1	Specifies if the OPUS codec capability of the phone is enabled or disabled. Value Operation: • 0: Disabled. • 1: Enabled OPUS wideband with bitrate of 20KBps. • 2: Enabled OPUS narrowband with bitrate of 16KBps. • 3: Eanbled OPUS narrowband with bitrate of 12KBps. **Note:** Avaya J129 IP Phone does not support third-party local call conference with OPUS.
ENABLE_PHONE_LOCK	0	Specifies whether the **Lock** softkey and lock feature button are enabled on the phone. If you enable the parameter, then a user can lock the phone by pressing the button or selecting the feature. Value Operation: • 0: Disabled. **Lock** softkey and feature button are not displayed. • 1: Enabled. **Lock** softkey and feature button are 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.

Table continues…

Parameter name	Default value	Description
		• 1: Proxy server information received from PPM is not used.
ENABLE_PRESENCE	1	Specifies if presence will be supported. Value Operation: • 0: Disabled • 1: Enabled **Note:** This parameter is set to 0 in IP Office environment.
ENABLE_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 whether an **Emergency** softkey, with or without a confirmation screen, is displayed when the phone is registered. All emergency numbers are always supported. Value Operation: • 0: **Emergency** softkey is not displayed. • 1: **Emergency** softkey is displayed without a confirmation screen. • 2: **Emergency** softkey is displayed with a confirmation screen. **Note:** The parameter is set to 0 for IP Office environment.
ENABLE_SHOW_EMERG_SK_UNREG	2	Specifies whether an **Emergency** softkey, with or without a confirmation screen, is displayed when the phone is not registered.

Table continues…

Parameter name	Default value	Description
		All emergency numbers will always be supported. Value Operation: • 0: **Emergency** softkey is not displayed. • 1: **Emergency** softkey is displayed without a confirmation screen. • 2: **Emergency** softkey is displayed with a confirmation screen. **Note:** The parameter is set to 0 for IP Office environment.
ENCRYPT_SRTCP	0	Specifies whether RTCP packets are encrypted or not. SRTCP is only used if SRTP is enabled using MEDIAENCRYTIONRTCP. ENCRYPT_SRTCP parameter controls RTCP encryption for RTCP packets exchanged between peers. RTCP packets sent to Voice Monitoring Tools are always sent unencrypted. Value Operation: • 0: SRTCP is disabled. • 1: SRTCP is enabled.
ENFORCE_SIPS_URI	1	Specifies if a SIPS URI must be used for SRTP. Value Operation: • 0: Not enforced • 1: Enforced
ENHDIALSTAT	1	Specifies if the algorithm defined by the parameter is used during certain dialing behaviors. Value Operation: • 0: Disables algorithm. • 1: Enables algorithm, but not for contacts. • 2: Enables algorithm including contacts. **Note:** The parameter is set to 0 for IP Office environment.
EVENT_NOTIFY_AVAYA_MAX_USERS	20	Specifies the maximum number of users to be included in an event notification message from CM/AST-II or Avaya Aura® Conferencing 6.0 or later.

Table continues…

Parameter name	Default value	Description
		Valid values are 0 through 1000. This parameter is used only for development and debugging purposes.
EXCHANGE_AUTH_USERNAME_FORMAT	0	Specifies the necessary format of the username for http authentication. Value operation: • 0: Current format. Username= <ExchangeUserDomain\ExchangeUserAccount> or Username= <ExchangeUserAccount> if <ExchangeUserDomain> is empty. • 1: Office 365 format. Username= <ExchangeUserAccount@ExchangeUserDomain> or Username= <ExchangeUserAccount> if <ExchangeUserDomain> is empty.
EXTEND_RINGTONE	Null	Provides a way to customize ring tone files. This is a comma separated list of file names in xml format.
F		
FAILED_SESSION_REMOVAL_TIMER	30	Specifies the number of seconds the phone displays a session line appearance and generates re-order tone after an invalid extension is dialed and user does not press the **End Call** softkey. Valid values are 5 through 999.
FQDN_IP_MAP	Null	Specifies a comma separated list of name or value pairs where the name is an FQDN and the value is an IP address. The IP address may be IPv6 or IPv4 but the value can only contain one IP address. String length is up to 255 characters without any intervening spaces inside the string. The purpose of this parameter is to support cases where the server certificate Subject Common Name of Subject Alternative Names includes FQDN, instead of IP address, and the SIP_CONTROLLER_LIST is defined using IP address. This parameter is supported with phone service running over TLS, however, the main use case is for Avaya Aura SM/PPM services. This parameter must not to be used as an alternative to a DNS lookup or reverse DNS lookup.
G		

Table continues…

Parameter name	Default value	Description
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. 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.

Table continues…

Parameter name	Default value	Description
HTTPPROXY	Null	Specifies the address of the HTTP proxy server used by SIP phones to access an SCEP server that is not on the enterprise network. Valid value can contain zero or one IP address in dotted decimal or DNS name format, optionally followed by a colon and a TCP port number. The value can contain 0 to 255 characters.
HTTPSRVR	Null	Specifies zero or more HTTP server IP addresses to download configuration script files. The addresses must be separated by commas without any intervening spaces. The format of specifying IP addresses are: • Dotted decimal • Colon-hex • DNS name The parameter can be set by using LLDP. Valid values contains 0 to 255 ASCII characters.
I		
ICMPDU		Specifies if ICMP Destination Unreachable messages are generated. Value Operation: • 0: No messages are generated. • 1: Limited port unreachable messages are generated. • 2: Protocol and port unreachable messages are generated.
ICMPRED		Specifies if received ICMP Redirect messages are processed. Value Operation: • 0: No • 1: Yes
INGRESS_DTMF_VOL_LEVEL	-12dBm	Specifies the power level of tone, expressed in dBm0. Values can range from -20dBm to -7dBm.
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.

Table continues…

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

Table continues…

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

Table continues…

Parameter name	Default value	Description
		Filenames can be full URL, relative pathname, or filename. Valid values can contain 0 to 1096 ASCII characters, including commas. Filenames must end in `.xml`
LLDP_ENABLED	2	Specifies whether LLDP is enabled. Value operation: • 0: Disabled • 1: Enabled • 2: Enabled, but only begins transmitting if an LLDP frame is received.
LOCAL_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 does not need to dial area code. • 1: User need to dial area code. When enabled, the area code parameter (PHNLAC) should also be configured. **Note:** This parameter is supported when the phone is failed over.
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. 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.

Table continues…

Parameter name	Default value	Description
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.
MAX_TRUSTCERTS	6	Specifies the maximum number of trusted certificates files defined by this parameter that can be downloaded to the phone. Valid values are from 1 to 10.
MEDIA_ADDR_MODE	4	Specifies the IP address of the endpoint when both IPv4 and IPv6 addresses are provided. This parameter is used for SIP signalling. Value operation: • 4: IPv4 • 6: IPv6 • 46: Prefer IPv4 over IPv6 • 64: Prefer IPv6 over IPv4
MEDIAENCRYPTION	9	Specifies which media encryption (SRTP) options is supported. 3 options are supported in a comma-separated list. Options must match to those specified in CM IP-codec-set form. • 1: aescm128-hmac80 • 2: aescm128-hmac32 • 3: aescm128-hmac80-unauth

Table continues…

Parameter name	Default value	Description
		• 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 publishes this list in the SDP-OFFER or chooses from SDP-OFFER list according to the list order defined in MEDIAENCRYPTION. Avaya Aura® Communication Manager has the capability to change the list order in the SDP-OFFER (for audio only) when the SDP-OFFER is pass through.
MEDIA_NEG_PREFERENCE	0	Specifies the address family preference used by a dual mode answer in non-Avaya environment. This parameter is not applicable for single mode phones. Value operation: • 0: Remote or offerer's preference • 1: Local
MUTE_ON_REMOTE_OFF_HOOK	0	Controls the speakerphone muting for a remote-initiated (a shared control or OOD-REFER) speakerphone off-hook. Value Operation: • 0: The speakerphone is unmuted. • 1: The speakerphone is muted. The value is applied to the phone only when the phone is deployed with a Avaya Aura® Communication Manager 6.2.2 and earlier releases. If the phone is deployed with Avaya Aura® Communication Manager 6.3 or later, the setting is ignored. Instead the feature is delivered through PPM. The Turn on mute for remote off-hook attempt parameter is enabled in the station form through the Avaya Aura® Session Manageror

Table continues…

Parameter name	Default value	Description
		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	CAIdentifier	Specifies an identifier for the CA certificate with which the SCEP certificate request is to be signed, if the server hosts multiple Certificate Authorities. The value can contain zero to 255 ASCII characters. The parameter is only available in an Avaya Aura® environment.
MYCERTCN	$SERIALNO	Specifies the Common Name (CN) used in the SUBJECT of an SCEP certificate request. The value must be a string that contains either $SERIALNO" (which will be replaced by the phone's serial number) or $MACADDR (which will be replaced by the phone's MAC address), but it can contain other characters as well, including spaces. The value can contain eight ($MACADDR) to 255 characters.
MYCERTDN	Null	Specifies the part the SUBJECT of an SCEP certificate request that is common for all phones. The value must begin with a / and can include Organizational Unit, Organization, Location, State and Country. The value can contain Zero to 255 ASCII characters. **Note:** / must used as a separator between components. Commas do not work with some servers

Table continues…

Parameter name	Default value	Description
MYCERTKEYLEN	2048	Specifies the bit length of the public and private keys generated for the SCEP certificate request. The value is a 4 ASCII numeric digits. The phone supports only value 2048.
MYCERTRENEW	90	Specifies the percentage of the identity certificate's validity interval after which renewal procedure is initiated. Valid values are 1 through 99.
MYCERTURL	Null	Specifies the URL of the SCEP server for obtaining an identity certificate. The URL can be HTTP or HTTPS. The valid values can range from Zero to 255 ASCII characters.
MYCERTWAIT	1	Specifies the phone's behavior if the SCEP server indicates that the certificate request is pending for manual approval. Value Operation: • 0: Poll the SCEP server periodically in the background. • 1: Wait until a certificate is received or the request is rejected.
N		
NO_DIGITS_TIMEOUT	20	Specifies the number of seconds the phone waits for a digit to be dialed after going off-hook and before generating a warning tone. Valid values are 1 through 60.
O		
OCSP_ACCEPT_UNK	1	Specifies whether in cases where certificate revocation status for a specific certificate cannot be determined to bypass certificate revocation operation for this certificate. Value operation: • 0: Certificate is considered to be revoked if the certificate revocation status is unknown. TLS connection will be closed. • 1: Certificate revocation operation will accept certificates for which the certificate revocation status is unknown.

Table continues…

Parameter name	Default value	Description
OCSP_CACHE_EXPIRY	2880	Specifies the time interval for the OCSP cache expiry in minutes. OCSP response cache expiry uses nextUpdate value in OCSP response message. If nextUpdate is not present, then OCSP_CACHE_EXPIRY parameter value is used. Valid range is from 60 to 10080
OCSP_ENABLED	0	Specifies that OCSP is used to check the revocation status of the certificates. Value operation: • 0: Disabled. Certificate revocation checking is not performed. • 1: Enabled. Certificate revocation checking is performed.
OCSP_HASH_ALGORITHM	0	Specifies the hashing algorithm for OCSP request. Value operation: • 0: SHA1 hash algorithm • 1: SHA256 hash algorithm
OCSP_NONCE	1	Specifies whether a nonce is added in OCSP requests and expected in OCSP responses. Value operation: • 0: Not added to OCSP request. • 1: Added to OCSP request.
OCSP_TRUSTCERTS		Specifies a comma separated list of OCSP trusted certificates that are used as OCSP signing authority for checking the revocation status of the certificate. This applies to when the OCSP responder is using a different CA. Spaces are not permitted in this parameter.
OCSP_URI	Null	Specifies the URI of an OCSP responder. The URI can be an IP address or hostname. Valid values contain 0 to 255 ASCII characters, zero or one URI.
OCSP_USE_CACHE	1	Specifies that the OCSP caching is in use. Value operation: • 0: OCSP is not used. Always check with OCSP responder. • 1: OSCP cache caching is used.

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: Use the OCSP_URI and then the OCSP field of the Authority Information Access (AIA) extension of the certificate. • 2: Use 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		
PHNCC	1	Specifies the country code for United States. The value is 1. Valid values 1 through 999.
PHNDPLENGTH	5	Specifies the internal extension number length. If your extension is 12345, and your dial plan length is 5. The maximum extension length is 13. This value must match the extension length set on your call server. Valid values are 3 through 13.
PHNEMERGNUM	Null	Specifies an emergency phone number to be dialed if the associated button is selected. Valid values can contain up to 30 dialable characters (0 to 9, *, #).
PHNMOREEMERGNUMS	Null	Specifies list of emergency numbers separated by comma. Valid values may contain up to 30 dialable characters (0 to 9, *, #).
PHNIC	011	Specifies the international access code

Table continues…

Parameter name	Default value	Description
		For the United States, the value is 011. Valid values are from 0 to 4 dialable characters (0-9,*,#).
PHNLAC		Phone's Local Area Code indicates the phone's local area code, which along with the parameter LOCAL_DIAL_AREA_CODE, allows users to dial local numbers with more flexibility. PHNLAC is a string representing the local area code the phone. **Note:** This parameter is supported when the phone is failed over.
PHNLD	1	Specifies the long distance access code Valid values are 0 through 9 and empty string. If long distance access code is not needed then set the parameter to null.
PHNLDLENGTH	10	Specifies the national phone number length. For example, 800-555-1111 has a length of 10. Valid values are 5 through 15.
PHNMUTEALERT_BLOCK	1	Specifies if the **Mute Alert** feature is blocked or unblocked. Value Operation: • 0: Unblocked • 1: Blocked
PHNNUMOFSA	3	Specifies the number of session appearances the phone must support while operating in a non-Avaya environment. Valid values are 1 through 10.
PHNOL	9	Specifies the outside line access code. This is the number you press to make an outside call. Valid values are 0 to 2 dialable characters (0-9, *, #).
PHONE_LOCK_IDLETIME	0	Specifies the interval of idle time, in minutes, after which the phone will automatically lock. The phone will lock irrespective of the value of ENABLE_PHONE_LOCK.
PHY1STAT	1	Specifies the speed and duplex settings for the Ethernet line interface.

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. The parameter is not supported when VLANSEPMODE is 1. Valid values are 0 through 7.
PHY2STAT	1	Specifies the speed and duplex settings for the secondary (PC) Ethernet interface. Value Operation: • 0: disabled • 1: auto-negotiate • 2: 10Mbps half-duplex • 3: 10Mbps full-duplex • 4: 100Mbps half-duplex • 5: 100Mbps full-duplex • 6: 1Gbps full-duplex, if supported by hardware, otherwise auto-negotiated
PHY2TAGS	0	Determines whether or not VLAN tags are stripped on Ethernet frames going out of the Computer (PC) port. Value Operation: • 0: Strip tags. VLAN tags are stripped from Ethernet frames leaving the computer (PC) port of the phone.

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:** The parameter is configured through the following: • SET command in a settings file • LLDP
PKCS12URL	Null	Specifies the URL to be used to download a PKCS #12 file containing an identity certificate and its private key. Valid values contain 0 to 255 ASCII characters, zero or one URL. The value can be a string that contains either $SERIALNO or $MACADDR, but it may contain other characters as well. If $MACADDR is added to the URL, then the PKCS12 filename on the file server includes MAC address without colons. PKCS12 file download is preferred over SCEP if PKCS12URL is defined.
PKCS12_PASSWD_RETRY	3	Specifies the number of retries for entering PKCS12 file password. If user failed to enter the correct PKCS12 file password after PKCS12_PASSWD_RETRY retries, then the phone will continue the startup sequence without installation of PKCS12 file. Valid values are from 0 to 100. Value operation: • 0: No retry
PLAY_TONE_UNTIL_RTP	1	Specifies whether locally-generated ringback tone stops as soon as SDP is received for an early media session, or whether it will continue until RTP is actually received from the far-end party.

Table continues…

Parameter name	Default value	Description
		Value Operation: • 0: Stop ringback tone as soon as SDP is received. • 1: Continue ringback tone until RTP is received (default).
POE_CONS_SUPPORT		Enables power over Ethernet conservation mode. Value Operation: • 0: Power conservation mode is not supported. • 1: Power conservation mode is supported.
PROCPSWD	27238	Specifies an access code to access the admin menu procedures. Valid values contain 0 through 7 ASCII numeric digits. The default value is 27238 unless indicated otherwise below. A null value implies that an access code is not required for access. **Note:** • Setting this parameter through PPM is more secure because this file can usually be accessed and read by anyone on the network. Setting the value in this file is intended primarily for configurations with versions of phone or if server software that do not support setting this value from the server. • For enhanced security, use ADMIN_PASSWORD instead of PROCPSWD.
PROCSTAT	0	Specifies an access code to access the admin menu procedures. Value Operation: • 0: Local procedures can be used (default). • 1: Local procedures cannot be used.
PROVIDE_LOGOUT		Specifies if user can log out from the phone. Value Operation: • 0: No • 1: Yes

Table continues…

Parameter name	Default value	Description
		Note: This parameter is set to 0 in IP Office environment.
PROVIDE_NETWORKINFO_SCREEN		Specifies if the **Network Information** menu is displayed on the phone. Value Operation: • 0: No • 1: Yes
PROVIDE_OPTIONS_SCREEN		Specifies if **Options & Settings** menu is displayed on phone. Value Operation: • 0: No • 1: Yes
PROVIDE_TRANSFER_TYPE	0	Provides the call transfer type in 3rd party environments. Value 0 or 1.
PSTN_VM_NUM		Specifies the dialable string that is used to call into the messaging system. For example, when you press the **Message Waiting** button. **Note:** This parameter is supported when the phone is failed over.
Q		
R		
RDS_INITIAL_RETRY_ATTEMPTS	15	Specifies the number of retries after which the phone abandons its attempt to contact the PPM server. Valid values are 1 through 30.
RDS_INITIAL_RETRY_TIME	2	Specifies the number of seconds that the phone waits for the first time before trying to contact the PPM server again after a failed attempt. Each subsequent retry is delayed by double the previous delay. Valid values are 2 through 60.
RDS_MAX_RETRY_TIME	600	Specifies the maximum delay interval in seconds after which the phone abandons its attempt to contact the PPM server. Valid values are 2 through 3600.

Table continues…

Parameter name	Default value	Description
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. • 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.
REDIRECT_TONE	1	Specifies the tone to play when a call goes to coverage. Valid values are from 1 to 4.

Table continues…

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

Table continues…

Parameter name	Default value	Description
		XR) (RFC 3611) is sent as part of the RTCP packets to remote peer or to RTCP monitoring server. Value Operation: • 0: No • 1: Yes
RTCPCONT		Specifies if the sending of RTCP is enabled. Value Operation: • 0: No • 1: Yes
RTCPMON	Null	Specifies the IP or DNS address for the RTCP monitor. You can set this parameter only if the environment is not an Avaya environment. The values can range from 0 through 255 characters.
RTCPMONPERIOD	5	Specifies the interval, in seconds, for sending out RTCP monitoring reports. Valid values are from 5 to 30 seconds.
RTCPMONPORT	5005	Specifies the RTCP monitor port number. You can set this parameter only if the environment is not an Avaya environment. The values can range from 0 through 65535. Default is 5005.
RTP_PORT_LOW		Specifies the lower limit of the UDP port range to be used by RTP or RTCP and SRTP or SRTCP connections. The values can range from 1024 through 65503.
RTP_PORT_RANGE		Specifies the range or number of UDP ports available for RTP or RTCP and SRTP or SRTCP connections This value is added to RTP_PORT_LOW to determine the upper limit of the UDP port range. The values can range from 32 through 64511.
S		
SCEPPASSWORD	$SERIALNO	Specifies the password to be included in the challengePassword attribute of an SCEP certificate request. Values can contain 0 to 32 ASCII characters (50 ASCII characters.

Table continues…

Parameter name	Default value	Description
		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.
SEND_DTMF_TYPE	2	Specifies if DTMF tones are sent in-band as regular audio, or out-of-band using RFC 2833 procedures. Value Operation: • 1: In-band • 2: Out-of-band
SERVER_CERT_RECHECK_HOURS	24	Specifies the number of hours after which certificate expiration and OCSP will be used, if OCSP is enabled, to recheck the revocation and expiration status of the certificates that were used to establish a TLS connection. Valid values are from 0 to 32767. Value operation: • 0: Periodic checking is disabled.
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	Null	Specifies a list of SIP controller designators, separated by commas without any spaces. Controller designator has the following format:

Table continues…

Parameter name	Default value	Description
		host[:port][;transport=xxx], where host is an proxy address in dotted-decimal or DNS name format. In third-party call control setup, only DNS format is supported. [:port] is an optional port number. [;transport=xxx] is an optional transport type In third-pary call control setup, only one SIP controller is supported.
SIP_CONTROLLER_LIST_2	Null	Specifies the registration address. This parameter replaces SIP_CONTROLLER_LIST for dual mode phones. The parameter contains a comma separated list of SIP proxy or registrar servers. The list has the following format: host[:port][;transport=xxx].
SIPCONFERENCECONTINUE	0	Specifies if a conference call continues after the host hangs up. Value Operation: • 0: Drop all parties. • 1: Continue conference **Note:** This parameter is set to 1 in IP Office environment.
SIPDOMAIN	Null	Specifies the domain name to be used during SIP registration. The value can contain 0 to 255 characters. The default value is null.
SIPPORT	5060	Specifies the port the phone opens to receive SIP signaling messages. Valid values are 1024 through 65535. The default value is 5060.
SIPSIGNAL	2	Specifies the type of transport used for SIP signaling. Value Operation: • 0: UDP • 1: TCP • 2: TLS
SLMCAP	0	Specifies if the SLA Monitor agent is enabled for packet capture.

Table continues…

Parameter name	Default value	Description
		Value Operation: • 0: Disabled (default) • 1: Enabled and payloads are removed from RTP packets • 2: Enabled and payloads are included in RTP packets • 3: Controlled from admin menu - Allows you to enable or disable of RTP packets capture using local admin procedures.
SLMCTRL	0	Specifies whether the SLA Monitor agent is enabled for phone control. Value Operation: • 0: Disabled • 1: Enabled • 2: Controlled from admin menu.
SLMPERF	0	Specifies whether the SLA Monitor agent is enabled for phone performance monitoring. Value Operation: • 0: Disabled • 1: Enabled
SLMPORT	50011	Specifies the UDP port that will be opened by the SLA Monitor agent to receive discovery and test request messages. Valid values are 6000 through 65535. The default value is 50011. ✱ **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.

Table continues…

Parameter name	Default value	Description
		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 • 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.

Table continues…

Parameter name	Default value	Description
		Addresses can be in dotted-decimal or DNS name format, separated by commas without any intervening spaces. The list can contain up to 255 characters.
SNTP_SYNC_INTERVAL	1440 minutes	Specifies the time interval, in minutes, during which the phone will attempt to synchronize its time with configured NTP servers. Valid values are from 60 to 2880 minutes.
SPEAKERSTAT	2	Specifies the operation of the speakerphone. Value Operation: • 0: Speakerphone disabled • 1: One-way speaker (also called monitor) enabled. • 2: Full (two-way) speakerphone enabled.
SSH_ALLOWED	2	Specifies if SSH is supported. Value Operation: • 0: Disabled • 1: Enabled • 2: Configured using local admin procedure. When this mode is configured, then by default the SSH server is disabled.
SSH_BANNER_FILE	Null	Specifies the file name or URL for a custom SSH banner file. If the value is null, english banner is used for SSH. The value can contain 0 to 255 characters.
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.

Table continues…

Parameter name	Default value	Description
		For IPO the recommended value shall be reg, message-summary, avaya-ccs-profile.
SUBSCRIBE_SECURITY		Specifies the use of SIP or SIPS for subscriptions. Value Operation: • 0: The phone uses SIP for both the request URI and the contactheader regardless of whether SRTP is enabled. • 1: The phone uses SIPS for both the request URI and the contact header if SRTP is enabled. TLS is on and MEDIAENCRYPTION has at least one valid crypto suite. • 2: SES or PPM does not show a FS-phoneData FeatureName with a Feature Version of 2 in the response to the getHomeCapabilities request. For IP office environment, the applicable values are 0 and 1.
SYMMETRIC_RTP	1	Specifies if the phone must discard received RTP or SRTP datagrams if their UDP source port number is not the same as the UDP destination port number included in the RTP or SRTP datagrams of that endpoint. Value Operation: • 0: Ignore the UDP source port number in received RTP/SRTP datagrams. • 1: Discard received RTP/SRTP datagrams if their UDP Source Port number does not match the UDP Destination Port number that the phone includes in RTP/SRTP datagrams intended for that phone.
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.

Table continues…

Parameter name	Default value	Description
		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. • 1: Keep-alive messages are sent (default).
TCP_KEEP_ALIVE_INTERVAL	10	Specifies the number of seconds that the telephone waits before re-transmitting a TCP keep-alive (TCP ACK) message. Valid values are from 5 through 60.
TCP_KEEP_ALIVE_TIME	60	Specifies the number of seconds that the telephone waits before sending out a TCP keep-alive (TCP ACK) message. Valid values are from 10 through 3600
TIMEFORMAT		Specifies the format for time displayed in the phone. Value Operation: • 0: AM or PM format. • 1: 24hour. 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.
TLSSRVR		Specifies zero or more HTTPS server IP addresses, which is used to download configuration script files. The IP addresses can be specified in dotted-decimal, or DNS name format separated by commas without any intervening spaces. Valid values contain 0 to 255 ASCII characters, including commas. This parameter can also be changed through LLDP.
TLSSRVRID	1	Specifies how a phone evaluates a certificate trust.

Table continues…

Parameter name	Default value	Description
		Value Operation: • 0: Identity matching is not performed. • 1: The certificate is trusted only if the identity used to connect to the server matches the certificate identity, as per Section 3.1 of RFC 2818. For SIP-TLS connections, an additional check is performed to validate the SIP domain identified in the certificate, as per RFC 5922. The parameter is configured through the `46xxsettings.txt` file.
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		
USBPOWER	2	Controls USB power when power is provided to the USB interface. Value operation: • 0: Turn off USB power regardless of power source. • 1: Turn on USB power only if Aux powered. • 2: Turn on USB power regardless of power source. • 3: Turn on USB power if Aux powered or PoE Class 3 power.
USER_STORE_URI		Specifies the URI path of IP Office for storing user data. **Note:** If the value of this parameter is set to null, then the addition, deletion, and modification of **Contacts** is disabled.
USE_QUAD_ZEROES_FOR_HOLD		Specifies how Hold will be signaled in SDP. Value Operation: • 1: “a=directional attributes" will be used • 0: "c=0.0.0.0" will be used
V		
VLANSEPMODE	1	specifies whether full VLAN separation will be enabled by the built-in Ethernet switch while the

Table continues…

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

Table continues…

Parameter name	Default value	Description
		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.
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.

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		

Table continues…

Title	Use this document to:	Audience
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® System Manager on Avaya Aura® System Platform at a customer site.
Avaya IP Office™ Platform SIP Telephone Installation Notes	See the installation procedures and initial administration information for IP Office SIP telephone devices.	For people who install, configure and verify SIP telephone devices on IP Office.
Administering		
Administering Avaya Aura® Session Manager	See information about how to perform Avaya Aura® Session Manager administration tasks including how to use management tools, how to manage data and security, an how to perform periodic maintenance tasks.	For people who perform Avaya Aura® Session Manager system administration tasks.
Administering Avaya Aura® System Manager	See information about how to perform Avaya Aura® System Manager administration tasks including how to use management tools, how to manage data and security, an how to perform periodic maintenance tasks.	For people who perform Avaya Aura® System Manager administration tasks.
Administering Avaya IP Office™ Platform with Manager	See information about short code configurations for the feature list	For people who need to access IP Office features using short codes.
Administering Avaya IP Office™ Platform with Web Manager	See information about IP Office Web Manager administration tasks including how to use the management tool, how to manage data and security, and how to perform maintenance tasks.	For people who perfrom IP Office Web Manager administration tasks.
Maintaining		

Table continues…

Title	Use this document to:	Audience
Maintaining Avaya Aura® Session Manager	See information about the maintenance tasks for Avaya Aura® Session Manager.	For people who maintain Avaya Aura® Session Manager.
Troubleshooting Avaya Aura® Session Manager	See information for troubleshooting Avaya Aura® Session Manager, resolving alarms, replacing hardware, and alarm codes and event ID descriptions.	For people who troubleshoot Avaya Aura® Session Manager.
Using Avaya IP Office™ Platform System Status Application	See information about the maintenance tasks for System Status Application.	For people who maintain System Status Application.
Using Avaya IP Office™ Platform System Monitor	See information about the maintenance tasks for SysMonitor.	For people who maintain SysMonitor.

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

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.

Index