Installing and Administering Avaya 9608/9611G/9621G/9641G/9641GS IP Deskphones SIP

Release 7.1.15
Issue 4
January 2023

Note

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

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

Heritage Nortel Software

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

Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

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

T9 Text Input and other products are covered by one or more of the following patents: U.S. Pat. Nos. 5,187,480,5,818,437, 5,945,928, 5,953,541, 6,011,554, 6,286,064, 6,307,548, 6,307,549, and 6,636,162,6,646,573, 6,970,599; Australia Pat. Nos. 727539, 746674, 747901; Austria Pat. Nos. AT225534, AT221222; Brazil P.I. No. 9609807-4; Canada Pat. Nos. 1,331,057, 2,227,904,2,278,549, 2,302,595; Japan Pat. Nos. 3532780, 3492981; United Kingdom Pat. No. 2238414B; Hong Kong Standard Pat. No. HK1010924; Republic of Singapore Pat. Nos. 51383, 66959, 71979; European Pat. Nos. 1 010 057 (98903671.0), 1 018 069 (98950708.2); Republic of Korea Pat. Nos. KR201211B1, KR226206B1, 402252; People's Republic of China Pat. No. ZL96196739.0; Mexico Pat. Nos. 208141, 216023, 218409; Russian Federation Pat. Nos. 2206118, 2214620, 2221268; additional patent applications are pending

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of

support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Regulatory Statements

Australia Statements

Handset Magnets Statement:

Danger:

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

Industry Canada (IC) Statements

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.

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

Japan Statements

Class B Statement

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

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

Denan Power Cord Statement

Danger:

Please be careful of the following while installing the equipment:

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

警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

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

México Statement

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

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

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

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

Brazil Statement

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

Power over Ethernet (PoE) Statement

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

Taiwan Low Power Radio Waves Radiated Devices Statement

802.11b/802.11g/BT:

Article 12 — Without permission granted by the NCC, any company, enterprise, or user is not allowed to change frequency, enhance transmitting power or alter original characteristic as well as performance to an approved low power radio-frequency devices.

Article 14 — The low power radio-frequency devices shall not influence aircraft security and interfere legal communications; If found, the user shall cease operating immediately until no interference is achieved. The said legal communications means radio communications is operated in compliance with the Telecommunications Act. The low power radio-frequency devices must be susceptible with the interference from legal communications or ISM radio wave radiated devices.

低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

U.S. Federal Communications Commission (FCC) Statements

Compliance Statement

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

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

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

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

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 https://support.avaya.com or Avaya Inc., 2605 Meridian Parkway Suite 200. Durham, NC 27713 USA.

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

General Safety Warning

- Use only the Avaya approved Limited Power Source power supplies specified for this product.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

This document contains information about how to install and deploy 9600 Series IP Deskphones. It provides administration information for only the following 9600 Series IP Deskphones models:

- 9608
- 9608G
- 9611G
- 9621G
- 9641G
- 9641GS

This document is intended for people who install and maintain the 9600 Series IP Deskphones. For example, administrators and service engineers.

Change history

Date	Summary of changes
August 2022	Updated Phone administration chapter
February 2022	Updated Phone administration chapter
July 2021	Updated Security chapter
April 2021	Updated Phone administration chapter Updated List of configuration parameters
October 2020	Updated Phone administration chapter
June 2020	Added LDAP Directory topic
January 2020	Updated the Data Privacy Controls Addendum chapter
October 2019	Updated Phone administration chapter Updated List of configuration parameters

Chapter 2: 9600 Series IP Deskphones overview

9600 Series IP Deskphones overview

Avaya 9600 Series IP Deskphones is a set of desk handset devices that you can use for unified communication. These deskphones leverage the enterprise IP network and eliminate the need for a separate voice network. 9600 Series IP Deskphones work with the Avaya Aura® environment to provide a flexible architecture that works with your investments and accommodates growth as your business needs change.

These deskphones offer high audio quality and low power requirements and the flexibility to customize. With the high-performance phones of this series that can operate in both the H.323 and the Session Initiation Protocol (SIP) environments, you can use the phones to:

- Make conference calls more efficient and enhance customer interactions.
- Gain access to information quickly through easy-to-read and high-resolution displays.
- Speed up completion of common telephony tasks by using prompts on touch screens.
- Improve productivity with context-sensitive graphical interfaces that enhance call control and call management.
- Create a survivable, scalable infrastructure that delivers reliable performance and flexible growth as business needs change.
- Increase performance by deploying Gigabit Ethernet within your infrastructure.
- Reduce energy costs by using efficient Power-over-Ethernet (POE), including the sleep mode, that lowers energy consumption dramatically.

9600 Series IP Deskphones models

Deskphone model	Description
9608/9608G	You can use up to eight lines for the deskphone. The deskphone supports a traditional user interface and a graphical monochrome display. The 9608 has a built in 10/100 Ethernet switch, and the 9608G has an integrated Gigabit.
9611G	The 9611G has a traditional user interface and a graphical color display. You can use up to eight lines with the 9611G deskphone. The 9611G deskphone has an integrated Gigabit and a USB interface. The deskphone has a graphical color display with a white backlight.
9621G	The 9621G IP deskphone provides gigabit capability and touch screen functionality. Customers with a need for gigabit connectivity to the desktop prefer the 9621G deskphone.
9641G/9641GS	The 9641G/9641GS deskphone provides advanced capabilities with a color touch screen, wideband speaker, USB interface, Bluetooth® enabled headset support, and gigabit connectivity to the desktop. Customers who require gigabit capability for the desktop and the option to add more advanced capabilities prefer the 9641G/9641GS deskphone.

New in this release

Security enhancements

- Supports OpenSSL FIPS 140-2 certified cryptographic algorithms.
- Supports IPv6.
- Supports OpenSSL FIPS 140-2 certified cryptographic algorithms
- Supports Department of Defense solution deployment with Joint Inter-operability Test Command (JITC) compliance.
- Supports display of SSH fingerprint in the Administration menu.
- Displays version of OpenSSH and OpenSSL in the Administration menu.
- Supports SHA2 hash algorithm and strong encryption (256 bit symmetric and RSA 2048 and 4096 bit asymmetric keys) in TLS mode.
- Supports SRTP/SRTCP and TLS v1.2.
- Supports Enhanced Avaya Services Login (EASG) feature where an administrator can escalate to root privileges using an authentication file.

IPv6 and related features

- Supports ICMPv6, PPMv6, and DHCPv6.

- SIP registration over IPv4 and IPv6.
- Supports call features and MDA devices with ANAT and non-ANAT phones.
- Supports early media, delayed media, and media reshuffling with ANAT.

AS-SIP features

- Supports Multiple Level Precedence and Preemption, DSCP, and Blind Transfer as part of the AS-SIP feature.

Chapter 3: Initial setup and connectivity

Hardware and software prerequisites

Check the prerequisites to ensure that you have the required software and hardware before you install the 9600 Series IP Deskphones.

Hardware prerequisites

Ensure that the LAN:

- Uses Ethernet Cat. 5e or Cat. 6 cabling
- Has either of the following specifications:
  - IEEE 802.3af PoE
  - IEEE 802.3af PoE injector

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 .
- 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.

Installation checklist

Use the following checklist to see the tasks that you must perform to setup and connect the9600 Series IP Deskphones.

No.	Task	Reference	✔
1.	Check the prerequisites.	See *Prerequisites* topic for more information.	
2.	Collect the configuration data for the Deskphone, File Server, Network Server/ Switch (LLDP), Avaya Aura® System Manager, and DHCP Server.	See *Configuration through DHCP*, *File Server configuration*, and *Configuration through LLDP* topics for more information.	
3.	Configure the File Server, DHCP, and Network Server/Switch (LLDP).	See *Configuration through DHCP*, *File Server configuration*, and *Configuration through LLDP* topics for more information.	
4.	Create user, session, and communication profile on Avaya Aura® System Manager	See*Administering Avaya Aura® System Manager* guide for more information.	
5.	Download and install Avaya Aura® System Manager certificates on the phone.	See*Administering Avaya Aura® System Manager* guide for more information.	
6.	Unpack and assemble the deskphone components.		
7.	Connect the 9600 Series IP Deskphones to the power source and network.	See *Plugging in the deskphone* for more information.	

Administration methods

You can use the following methods to administer the devices. The following table lists the configuration parameters that you can administer through each of the corresponding methods.

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

Table continues…

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

Precedence of administration methods

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

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

Note:

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

Diagram: Phone deployment process

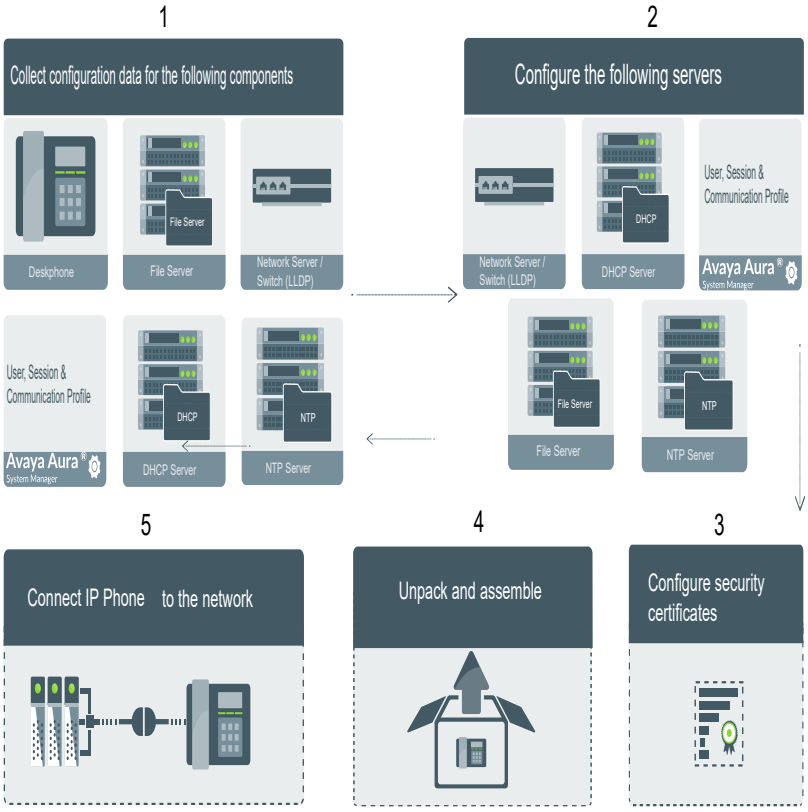
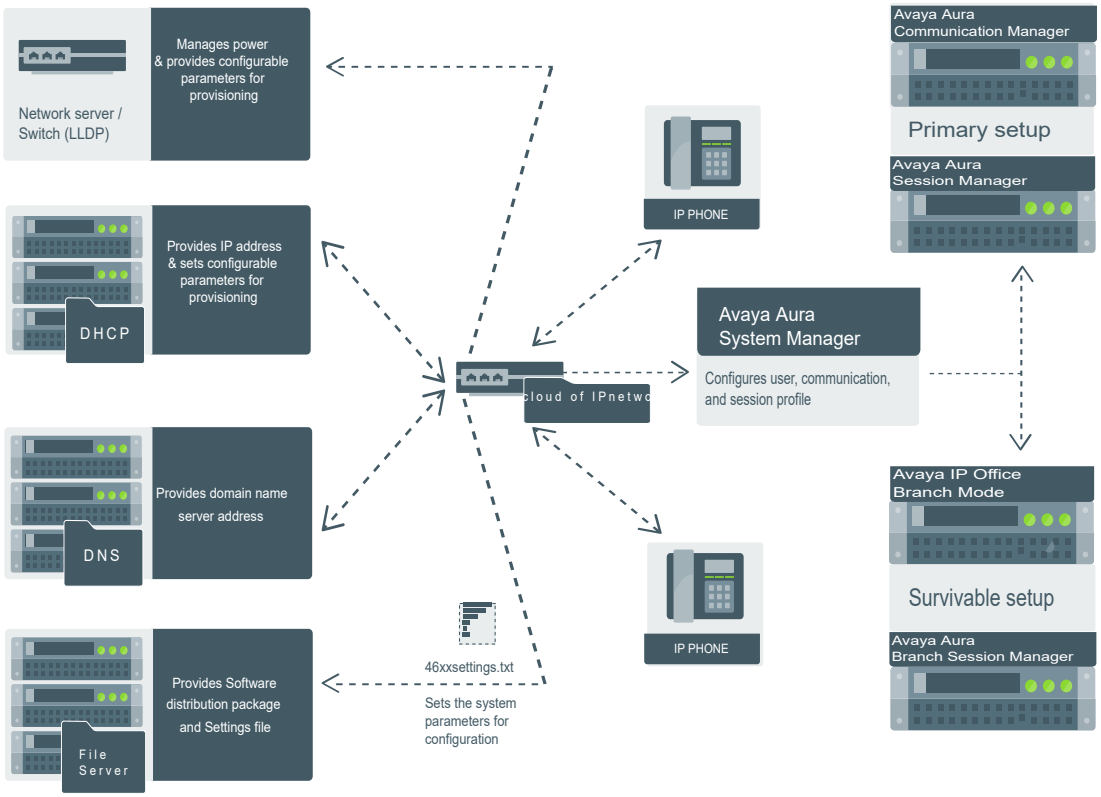


Diagram: IP phone setup



Provisioning server configuration block diagram

A provisioning server is an HTTP or an HTTPS server that the IP Phones connect to obtain the firmware files and configuration settings files.

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

The following block diagram depicts the provisioning server configuration:

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 9600 Series IP Deskphones Avaya J100 Series IP Phones use Type-Length-Value (TLV) elements specified in IEEE 802.1AB-2005, TIA TR-41 Committee - Media Endpoint Discovery (LLDP-MED, ANSI/TIA-1057), and Proprietary elements. LLDP Data Units (LLDPDUs) are sent to the LLDP Multicast MAC address.

The 9600 Series IP Deskphones Avaya J100 Series IP Phones running SIP software support IEEE 802.1AB if the value of the configuration parameter LLDP_ENABLED is “1” (On) or “2” (Auto). If the value of LLDP_ENABLED is “0” (off), the transmission and reception of Link Layer Discovery Protocol (LLDP) is not supported. When the value of LLDP_ENABLED is “2”, the transmission of LLDP frames does not begin until an LLDP frame is received. The first LLDP frame is transmitted within 2 seconds after the first LLDP frame is received. After transmission begins, an LLDPDU is transmitted every 30 seconds. A delay of up to 30 seconds in phone initialization might occur if the file server address is delivered by LLDP and not by DHCP.

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

By using LLDP, you can configure the following:

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

LLDPDU transmitted by the phones

Category	TLV Name (Type)	TLV Info String (Value)
Basic Mandatory	Chassis ID	IPADD of phone, IANA Address Family Numbers enumeration value for IPv4, or subtype 5:Network address.
Basic Mandatory	Port ID	MAC address of the device.
Basic Mandatory	Time-To-Live	120 seconds.
Basic Optional	System Name	The Host Name sent to the DHCP server in DHCP option 12.
Basic Optional	System Capabilities	Bit 2 (Bridge) will be set in the System Capabilities if the phone has an internal Ethernet switch. If Bit 2 is set in Enabled Capabilities then the secondary port is enabled.
Basic Optional	Management Address	Mgmt IPv4 IP address of device. Interface number subtype = 3 (system port). Interface number = 1. OID = SNMP MIB-II sysObjectID of the device.

Table continues…

Category	TLV Name (Type)	TLV Info String (Value)
IEEE 802.3 Organization Specific	MAC / PHY Configuration / Status	Reports auto negotiation status and speed of the uplink port on the device.
TIA LLDP MED	LLDP-MED Capabilities	Media Endpoint Discovery capabilities = 00-33 (Inventory, Power-via-MDI, Network Policy, MED Caps).
TIA LLDP MED	Network Policy	Tagging Yes/No, VLAN ID for voice, L2 Priority, DSCP Value.
TIA LLDP MED	Inventory – Hardware Revision	MODEL - Full Model Name.
TIA LLDP MED	Inventory – Firmware Revision	Firmware version.
TIA LLDP MED	Inventory – Software Revision	Software version or filename.
TIA LLDP MED	Inventory – Serial Number	Device serial number.
TIA LLDP MED	Inventory – Manufacturer Name	Avaya.
TIA LLDP MED	Inventory – Model Name	MODEL with the final Dxxx characters removed.
Avaya Proprietary	Call Server IP address	Call Server IP Address. Subtype = 3.
Avaya Proprietary	IP Phone addresses	Phone IP address, Phone Address Mask, Gateway IP Address. Subtype = 4.
Avaya Proprietary	File Server	File Server IP Address. Subtype = 6.
Avaya Proprietary	802.1Q Framing	802.1Q Framing = 1 if tagging or 2 if not.
Basic Mandatory	End-of-LLDPDU	Not applicable.

TLV impact on system parameter values

System parameter name	TLV name	Impact
PHY2VLAN	IEEE 802.1 Port VLAN ID	The value of the PHY2VLAN parameter on the phone is configured from the value of the Port VLAN identifier in the TLV.

Table continues…

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

Table continues…

System parameter name	TLV name	Impact
L2Q, L2QVLAN	TIA LLDP MED Network Policy (Voice Signaling)	L2Q - set to 2 (off) if T (the Tagged Flag) is set to 0 and to 1 (on) if T is set to 1. L2QVLAN - Set to the VLAN ID in the TLV. L2QAUD - Set to the Layer 2 Priority value in the TLV. DSCPAUD - Set to the DSCP value in the TLV. A check is made as to whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. This TLV is ignored if: • The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0. • The Application Type is not 1 (Voice) or 2 (Voice Signaling). • The Unknown Policy Flag (U) is set to 1.
SIP_CONTROLLER_LIST	Proprietary Call Server TLV	SIP_CONTROLLER_LIST will be set to the IP addresses 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	TLSSRVR and HTTPSRVR will be set to the IP addresses in this TLV value.
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.
POE_CONS_SUPPORT	Proprietary - PoE Conservation Level Request TLV	If the value of POE_CONS_SUPPORT is 1, POE_CONS_MODE is set to the level requested in the TLV.

Configuration through DHCP

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

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

You can configure the DHCP server to:

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

DHCP Site Specific Option

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

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

Following parameters can be configured with this feature:

Parameter	Description
ADMIN_PASSWORD	Specifies the security string used to access local procedures. The default is 27238. This is meant to replace PROCPSWD as it provides a more secure password syntax.

Table continues…

Parameter	Description
HTTPDIR	Specifies the path to the configurations and data files in HTTP and HTTPS GET operations during device bootup. This path is relative to the root of the HTTPS file server, to the directory in which the device configuration and data files are stored. If $MACADDR and/or $MODEL4 and/or $SERIALNO macro is present in the configured path then such macro is replaced with its actual value.The path may contain no more than 127 characters and may contain no spaces. HTTPDIR is the path for all HTTP operations. The command is `HTTPDIR=<path>`. In configurations where the upgrade and binary files are in the default directory on the HTTP server, do not use the `SET HTTPDIR=<path>`.
HTTPPORT	Sets the TCP port used for HTTP file downloads from non-Avaya servers. The default is 80.
HTTPSRVR	IP addresses or DNS names of HTTP file servers used for downloading settings, language, and firmware files during startup. 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. **Note:** Setting this parameter through PPM is more secure because this file can usually be accessed and read by anyone on the network.
PROCSTAT	Controls whether local (Admin menu) procedures can be used to configure the phone.
REUSETIME	Time in seconds for IP address reuse timeout, in seconds. The default is 60 seconds.
SIG	The signaling protocol download flag that indicates the protocol applied as follows: • 0 for Default • 1 for H.323 • 2 for SIP

Table continues…

Parameter	Description
SIP_CONTROLLER_LIST	SIP proxy or registrar server IP or DNS addresses that can be 0 to 255 characters, IP address in the dotted decimal name format, separated by commas and without any intervening spaces. The default is null, that is, no controllers.
TLSDIR	Specifies the path to the configurations and data files in HTTPS GET operations during device bootup. This path is relative to the root of the HTTPS file server, to the directory in which the device configuration and data files are stored. If $MACADDR and/or $MODEL4 and/or $SERIALNO macro is present in the configured path then such macro is replaced with its actual value. The string length can be from 0 to 127, without spaces.
TLSPORT	Destination TCP port used for requests to https server in the range of 0 to 65535. The default is 443, the standard HTTPS port.
TLSSRVR	IP addresses or DNS names of Avaya file servers used to download configuration files. Firmware files can also be downloaded using HTTPS. **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 auto generated. There is a provision where you can set up a different file server with your own custom Settings file.

DHCP options

You can configure the following options in the DHCP server:

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

Table continues…

Option	Description
Option 12	Avaya J100 Series IP Phones identify themselves to the DHCP server by sending the host name in Sub-Option 12 in `DHCP DISCOVER` and `DHCP REQUEST` options. The host name has the following format: `AVohhhhhh`, where: • `AV` stands for Avaya. • `o` is one of the following values based on Object Unique Identifier (OUI) derived from the first three octets of the phone MAC address: - A if OUI is 00-04-0D - B if OUI is 00-1B-4F - E if OUI is 00-09-6E - L if OUI is 00-60-1D - T if the OUI is 00-07-3B - X if the OUI is anything else • `hhhhhh` are the ASCII characters for the hexadecimal representation of the last three octets of the phone MAC address.
Option 15	Specifies the domain name. The domain name is required to resolve DNS names into IP addresses. Configure this option if you use a DNS name for the HTTP server. Otherwise, you can specify a domain as part of customizing the HTTP server. This domain name is appended to the DNS addresses specified in Option 6 before the phone attempts to resolve the DNS address. The phone queries the DNS address in the order they are specified in Option 6. If there is no response from an address, the phone queries the next DNS address. As an alternative to administering DNS by DHCP, you can specify the DNS server and domain name in the HTTP script file. If you use the script file, you must configure the DNSSRVR and DOMAIN parameters so that you can use the values of these parameters in the script. Administer Option 6 and Option 15 appropriately with DNS servers and domain names respectively.
Option 42	Specifies the SNTP IP address list. List servers in the order of preference. The minimum length is 4 and the length must be a multiple of 4.
Option 43	Specifies the encapsulated vendor-specific options that clients and servers use to exchange the vendor-specific information. Option 43 is processed only if the first code in the Option is 1 with a value of 6889. The value 6889 is an Avaya enterprise number. All values are interpreted as strings of ASCII characters that are accepted with or without a null termination character. Any invalid value is ignored and the corresponding parameter value is not set. Cannot be used simultaneously with DHCP SSON (Option 242).

Table continues…

Option	Description
Option 51	Specifies the DHCP lease time. If this option is not received, the DHCPOFFER is not accepted. Assign a lease time of six weeks or greater. If this option has a value of FFFFFFFF hex, the IP address lease is assumed to be infinite, so that the renewal and rebinding procedures are not necessary even if Options 58 and 59 are received. Expired leases causes the device to reboot.
Option 52	Specifies the overload option. If this option is received in a message, the device interprets the name and file parameters.
Option 53	Specifies the DHCP message type. The value can be one of the following: • 1 for DHCPDISCOVER • 3 for DHCPREQUEST For DHCPREQUEST sent to renew the device IP address lease: • If a DHCPACK is received in response, a log event record is generated with a Log Category of DHCP. • If a DHCPNAK is received in response, the device immediately ceases IP address usage, generates a log event record, sets IPADD to 0.0.0.0, and enters the DHCP INIT state.
Option 55	Specifies the parameter request list. Acceptable values are: • 1 for subnet mask • 3 for router IP addresses • 6 for domain name server IP addresses • 7 for log server • 15 for domain name • 26 for interface MTU • 42 for NTP servers
Option 57	Specifies the maximum DHCP message size. Set the value to 1500. Set the value to 1000.
Option 58	Specifies the DHCP lease renew time. If not received or if this value is greater than that for Option 51, the default value of T1, renewal timer is used.
Option 59	Specifies the DHCP lease rebind time. If not received or if this value is greater than that for Option 51, the default value of T2, rebinding timer is used.
Option 242	Specifies the site-specific option (SSON). It is optional but cannot be used simultaneously with Option 43. If you do not configure this option, ensure that one of the following parameters is configured appropriately elsewhere: • HTTPSRVR • TLSSRVR

DHCP vendor-specific option

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

Code	Parameter
1	Does not set any parameter. The value must be 6889.
2	HTTPSRVR
3	HTTPDIR
4	HTTPPORT
5	TLSSRVR
6	TLSDIR
7	TLSPORT
8	TLSSRVRID
9	L2Q
10	L2QVLAN
11	PHY1STAT
12	PHY2STAT
13	PROCSTAT
14	SIG
15	SIP_CONTROLLER_LIST

Extending use of DHCP lease

9600 Series IP Deskphones support configuration of network parameters using DHCP as per RFC 2131. However, when a DHCP server becomes unreachable and the DHCP lease currently held by the phone expires, the phone continues to use the same lease until the DHCP server becomes reachable. This functionality is controlled by setting the following parameter:

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

When this feature is enabled (DHCPSTD=1), the phone continues to use the lease data, including IP address, router and other options if the lease could not be renewed. In this state, the phone will attempt to reach a DHCP server every 60 seconds. When a DHCP server becomes available and a lease is renewed or new lease obtained, the phone performs a duplicate address detection on

the offered IP address. If no conflicts are detected, this IP address is assigned to the local network interface for use.

Parameter configuration through DHCP

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

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

The following parameters can be configured with this feature:

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

IPv4 and IPv6

- 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.

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

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

- IPv4 only mode.

The following table provides the results of the determination:

Table 1: IP Enablement Results

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

Note:

Do not configure IPv6 address manually, use auto-configuration instead.

Multiple Device Access

9600 Series IP Deskphones support Multiple Device Access (MDA) with which you can simultaneously register up to 10 SIP devices for one user. You can define the Maximum Simultaneous Device using the Avaya Aura® System Manager.

With MDA, the user can do the following:

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

  Alert other registered devices about an incoming call to your extension. When user answers a call on a device, the alerts on all the other devices stop. During the call, the other devices display an active call indicator on the call appearance for the active line.
- Be on multiple concurrent calls on different devices, but only one call on each device.

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

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

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

Related links

Shared Control on page 33
Multi-Device Access

Multi Device Access operation in dual-stack mode

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

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

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

Parameter	Description
SIP_CONTROLLER_LIST_2	Describes the list of SIP Proxy or Registrar servers separated by comma when the SIP device is configured for the dual-stack operation. Valid values are 0 to 255 characters in the dotted decimal or colon-hex format. The syntax is: `host[:port][;transport=xxx]` where • `host` is IP addresses in dotted-decimal format or hex format. • `[:port]` is the port number. The default values are 5060 for TCP and 5061 for TLS. • `[;transport=xxx]` is the transport type and `xxx` is either TLS or TCP. The default value is TLS. For example, `SIP_CONTROLLER_LIST_2="10.16.26.88:5060;transport=tcp"`

Table continues…

Parameter	Description
SIGNALING_ADDR_MODE	Describes the SIP registration over IPv4 or IPv6 and selects the preferred Avaya Aura® Session Manager for phones supporting the dual-stack mode. The Avaya Aura® Session Manager IP address is selected according to the parameter SIP_CONTROLLER_LIST_2. Valid values are: • 4: IPv4. This is the default value. • 6: IPv6

Shared Control

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

Note:

- SIP signaling must be set to TLS for the phone and the soft client. For security reasons, TCP is not supported with Shared Control.

Related links

Multiple Device Access on page 31

Configuring the File Server

About this task

Use this procedure to configure file server. Examples of File Server are as follows:

- Apache
- Internet Information Services (IIS)
- Avaya Utility Server

Procedure

1. Install the HTTP or HTTPS server software according to the vendor instructions.
2. Download and save the software distribution package and the settings file at the appropriate location on the server.
3. Unzip the distribution package and save the extracted files at an appropriate location on the server.

4. Open and modify the settings file to provision the required device configuration parameters.

Contents of the settings file

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

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

  Important:

  There must be space character between # and tag.
- Conditionals, of the form **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 Website.

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

- If the phone is unable to download J100Supgrade.txt file then all previously downloaded configuration is cached.

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

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
PROCSTAT	Y
PROCPSWD	Y
PHY1STAT	Y
PHY2STAT	Y
PHNCC	N
PHNDPLENGTH	N
PHNIC	N
PHNLDLENGTH	N

Table continues…

Parameter	Retained
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
WMLHOME	N
WMLPORT	N
WMLPROXY	N

Software distribution package

Software distribution package contains the files needed to operate the 9600 Series IP Deskphones packaged together in a ZIP format. You can download the package from the Avaya support website.

SIP software distribution package contains:

- One or more software files.
- One upgrade file (96x1Supgrade.txt).
- All of the display text language files.
- 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 deskphones based on the value of the TRUSTCERTS parameter. You must also include the System Manager route certificate in the TRUSTCERTS parameter for IM to work.
- File named release.xml that is used by the Avaya Software Update Manager application.
- The MIB file.

Note:

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

Two configuration files are important to understand. They are:

- The upgrade file, `96x1Supgrade.txt`, that tells the deskphone whether the deskphone needs to upgrade software. The deskphones 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`, which contains the option settings that enable, disable, or otherwise customize the settings you might need to tailor the deskphones for your enterprise.

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 Website to not get an old version.

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 .
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.

Powering the phone

The 9608, 9608G, 9611G, 9621G, 9641G and 9641GS phones are powered with the Global Single Port PoE Injector (GSPPOE-xx) and power module (DC power jack). The telephone power module is available and sold separately with the Comcode 700512602. Additionally, all phones support IEEE 802.3af-standard LAN-based power.

The power requirements and its class changes when you add peripherals such as button modules and USB devices. The power consumption of the drive varies and when the drive attempts to register with the phone, the phone determines if its current power class setting is adequate. Toggle the IEEE switch between L and H for providing adequate power. An auxiliary power supply is required when the power requirements is greater. Refer to the table below for different power requirements:

The impact of additional devices on power requirements over Ethernet Power Class

Phone Model	Default PoE (Class “L” on IEEE switch)	One BM12 (IEEE switch setting)	Two BM12s (IEEE switch setting)	Three BM12s (IEEE switch setting)	One SBM24 (IEEE switch setting)	Two SBM24s (IEEE switch setting)	Three SBM24s (IEEE switch setting)
9608	Class 1	L	H	H	L	H	H
9608G	Class 1	H	H	H	H	H	H
9611G	Class 1	H	H	H	H	H	H
9621G	Class 2	Not applicable; the 9621G does not support button modules or USB devices.					
9641G/ 9641GS	Class 2	H	H	H	H	H	H

Note:

- 9621G is a PoE Class 2 device with a 10/100/1000 switch and does not have an IEEE power switch.
- 9621G do not support a button module, a USB device, or a Dual Headset Adapter.
- The phone model 9608 does not support USB devices.
- If you set the IEEE switch on the back of the phone to H, the phone registers as a Class 3 device, even if the actual power usage is applicable to Class 1 or 2.
- Use the icons at the back of the phone for locating the correct jacks.
- The system parameter USBPOWER sets the power class for the USB interface.

To learn how to connect cords to the jacks on the phones:

Phone model	Figure:
9608, 9608G, 9611G	Connection jacks on a 9608, 9608G, or 9611G phone
9621G, 9641G, 9641GS	Connection jacks on a 9621G, 9641G, or 9641GS phone

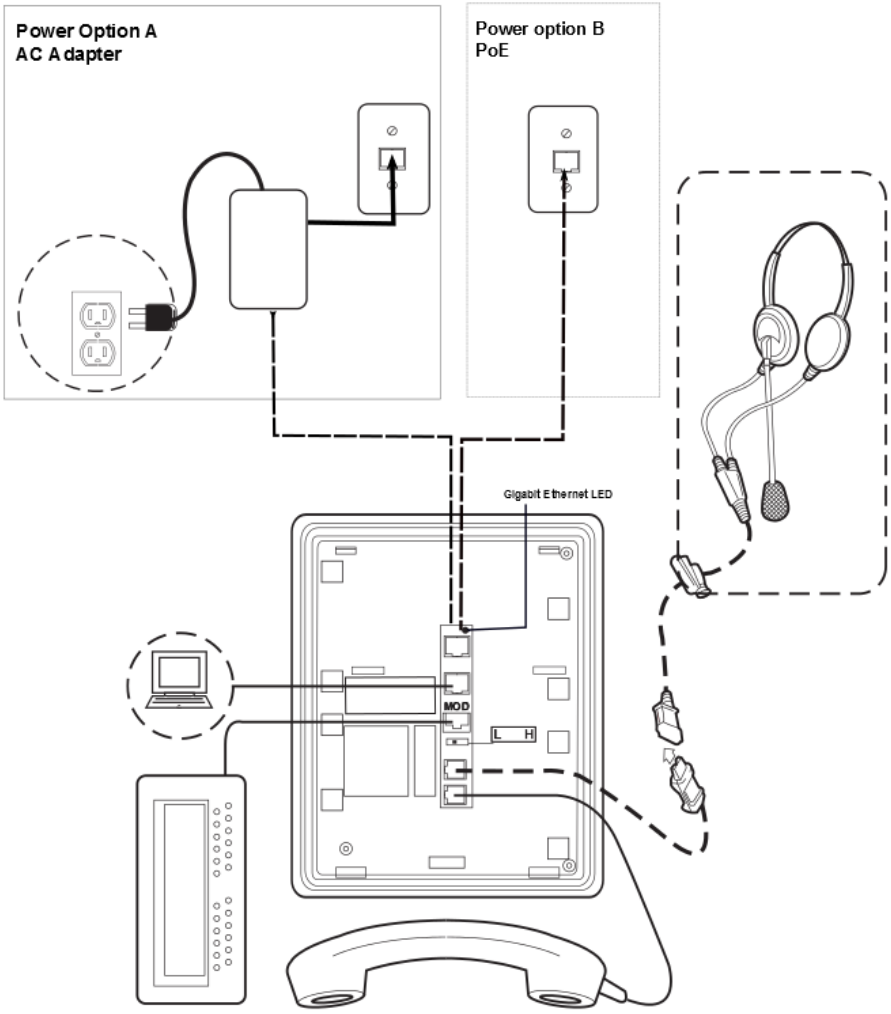
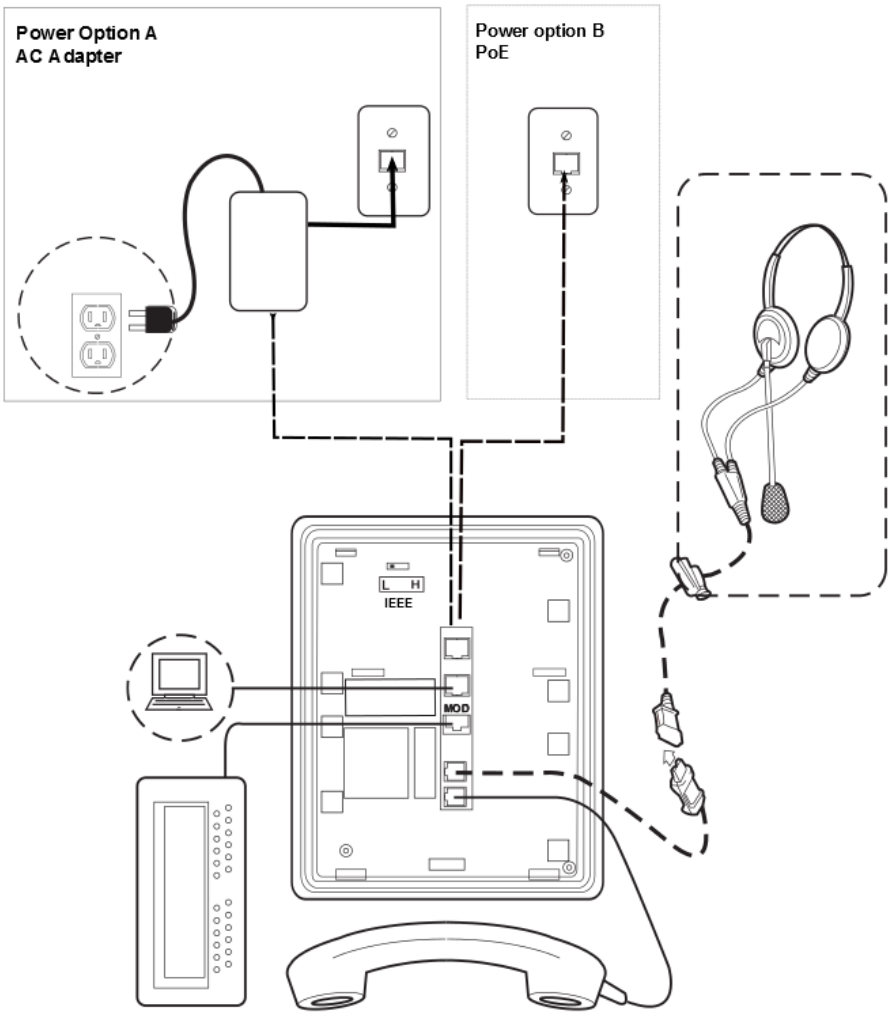


Figure 1: Connection jacks on a 9608, 9608G, or 9611G deskphone

Note:

The Gigabit Ethernet LED indicator is applicable to the 9608G and 9641GS IP phones. This indicator lights up steady green when a link of any speed is established, blinks with any network activity, and turns off upon the loss of network connectivity.

Figure 2: Connection jacks on a 9621G, 9641G, or 9641GS deskphone


Power Option A
AC Adapter
Power option B
PoE
L H
IEEE
MOD

Chapter 4: Security configurations

Security overview

SIP-based 9600 Series IP Deskphones provide several security features. The phone lock and user log out functionality protect the user privacy. When the phone is locked, a user can only receive calls or make emergency calls. User logs and data are protected with the user account.

9600 Series IP Deskphones support complex login password for protecting account privacy of both the user and the administrator. Login passwords can include both special and alphanumeric characters.

You can configure the following security features on the phones:

- Account management:
  - Storage of passwords and user credentials using Federal Information Processing Standards (FIPS 140–2)
  - FIPS 140-2 cryptographic algorithms for application, processes, and users
  - Control to toggle between FIPS and non-FIPS modes
  - Identity certificate installation using Simple Certificate Enrollment Protocol (SCEP) for enrollment and encrypted PKCS#12 file format to import both private key and certificate.
- Certificate management:
  - X509v3 compliant certificates
  - Public Key Infrastructure (PKI) for users who use third-party certificates for all Avaya services including 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.
- Control over USB power using system parameters.
- Display of SSH fingerprint 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.

Table continues…

Parameter name	Default value	Description
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 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.

USB port power

This feature is controls the power of the USB port. This feature is controlled by a parameter called USBPOWER. The available values for the parameter are:

- 0: Turns off the USB power.
- 1: Turns on the USB power only when it is powered through Aux.
- 2: Turns on the USB power.
- 3: Turns on the USB power when it is powered through Aux or PoE Class 3.

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

to establish mutual authentication. The server must validate the identity certificate to establish a secure connection.

Phones support three types of certificates:

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

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

You can use the following enhancements for installing identity certificates:

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

If the log level is maintained, the users are notified through a log message WARNING with the category CERTMGMT. The logs are maintained and displayed if SYSLOG is enabled.

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

Trusted certificates

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

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

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

Attribute Name	Description
endptIdentityCertIssuerName	Subject name of the issuer of the trusted certificate
endptIdentityCertSubjectName	Subject name of the trusted certificate
endptIdentityCertNotBefore	Valid from (date)
endptIdentityCertNotAfter	Valid until (date)
endptIdentityCertSN	Serial number of the trusted certificate
endptIdentityCertKeyUsageExtensions	Actions available for the trusted certificate
endptIdentityCertExtendedKeyUsage	Purpose of the trusted certificate
endptIdentityCertAltname	Subject Alternative Name (SAN) of the trusted certificate
endptIdentityCertFingerprint	SHA-1 hash of the trusted certificate (Displayed by HEX string)
endptIdentityCertBasicConstraints	Basic constraints of the trusted certificate

OCSP trust certificates

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

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

Phone identity certificates

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

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

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

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

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

Note:

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

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

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

Server certificate validation

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

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

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

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

Parameter name	Default value	Description
TLSSRVRID	1	Specifies how a phone evaluates a certificate trust . 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 address. For example, 192.168.1.2
- IPv6 address. For example, 2001:db8::2:1
- FQDN. For example, hostname.domain.com

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

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

1. Field of type IP address in the SAN extension

2. Full content of one field in the CN

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

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

Note:

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

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

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

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

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

Note:

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

Identity certificate renewal

9600 Series IP Deskphones support an enhanced feature to install or renew/replace[1] identity certificates before expiry. The enhanced certificate management feature introduces various improvements, such as:

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

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

- Quick renewal
  - Certificate renewal using the REST-based protocol to connect to Avaya Aura® System Manager.

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

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

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

Time for renewal

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

If you use the enhanced renewal feature, the parameter SCEPPASSWORD value must not be empty or set to a variable value such as $MACADDR or $SERIALNO. If you want to renew the certificate using the standard SCEP protocol, then remove the parameter SCEP_ENTITY_CLASS from the `46xxsettings.txt` file.

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

Expired certificate

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

Managing certificate CN and DN for renewal

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

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

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

Related links

Error handling and troubleshooting for certificate renewal on page 163

Configuration for secure installation

For secure installation, configure the following parameters.

Parameter	Set to	Notes
TRUSTCERTS		Provides the file names of certificates to be used for authentication. It supports both root and intermediate certificates and can contain up to six certificate files.
TLSSRVRID	1	Certificates installed on the servers must have the common name that matches the device configuration.
AUTH	1	Ensures usage of HTTPS file servers for configuration and software files download. Once AUTH is set to 1 and the device downloads the trusted certificates, the device can only download files from HTTPS server with certificates that can be validated using trusted certificate repository. You can change this parameter value back to 0 only by resetting the phone to defaults.
SSH_ALLOWED	0	Allows to keep SSH disabled.

SCEP parameters

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

Parameter	Type	Default value	Description
MYCERTURL	String	Null	Specifies the URL to access Simple Certificate Enrollment Protocol (SCEP) server. The device attempts to contact the server only if this parameter is set to other than its default value.
MYCERTCN	String	$SERIALNO	Specifies the Common name (CN) for SUBJECT in SCEP certificate request. The values can either be $SERIALNO or $MACADDR. If the value includes the string $SERIALNO, that string is be replaced by the phone's serial number. If the value includes the string $MACADDR, that string is be replaced by the phone's MAC address. In order to use enhanced certificate renewal in SMGR 8.1.3 and later, the value of MYCERTCN parameter must remain unchanged from the one used in existing identity certificate. Enhanced certificate renewal fails if this value is changed. If a new value is explicitly desired, then either remove the parameter SCEP_ENTITY_CLASS or remove the existing certificate by using DELETE_MY_CERT parameter and re-install a new one.

Table continues…

Parameter	Type	Default value	Description
MYCERTDN	String	Null	Specifies common part of SUBJECT in SCEP certificate request. This value defines the part of SUBJECT in a certificate request including Organizational Unit, Organization, Location, State, and Country that is common for requests from different devices. In order to use enhanced certificate renewal in SMGR 8.1.3 and later, the value of MYCERTDN parameter must remain unchanged from the one used in existing identity certificate. Enhanced certificate renewal fails if this value is changed. If a new value is explicitly desired, then either remove the parameter SCEP_ENTITY_CLASS or remove the existing certificate by using DELETE_MY_CERT parameter and re-install a new one.
MYCERTKEYLEN	Numeric	2048	Specifies the private key length in bits to be created in the device for a certificate enrollment. The range is from 1024 to 2048.
MYCERTRENEW	Numeric	90	Specifies the percentage of the identity certificate's validity interval after which renewal procedure will be initiated. The value is used to calculate the renewal time interval out of the device certificate’s Validity Object. If the renewal time interval has elapsed the phone starts to periodically contact the REST based protocol or SCEP server again to renew the certificate. The range is from 1 to 99. For example: if you set the MYCERTRENEW 90, certificate validity is 365 days, the renewal time is calculated as = (365)-(365*90%)= 36.5 days before the expiry. The phone starts using the new certificate immediately after the renewal, even when it is in use, for all new TLS connections. All existing connections are not broken.
MYCERTWAIT	Numeric	1	Specifies the behavior of the device when performing certificate enrolment. assign one of the following values: • 0: Periodical check in the background • 1: Wait until a certificate or a denial is received or a pending notification is received
MYCERTCAID	String	CAIdentifier	Specifies the Certificate Authority Identifier. Certificate Authority servers may require a specific CA Identifier string in order to accept GetCA requests. If the device works with such a Certificate Authority, the CA identifier string can be set through this parameter.

Table continues…

Parameter	Type	Default value	Description
SCEPPASSWORD	String	$SERIALNO	Specifies a challenge password to use with SCEP. The value of SCEPPASSWORD, if non-null, is included in a challengePassword attribute in SCEP certificate signing requests. If the value contains $SERIALNO, $SERIALNO is replaced by the value of SERIALNO. If the value contains $MACADDR, $MACADDR is replaced by the value of MACADDR without the colon separators. In order to use enhanced certificate renewal in SMGR 8.1.3 and later, SCEPPASSWORD value cannot be empty nor it can be set to a variable such as $MACADDR or $SERIALNO. If renewal or enrollment of a certificate is performed using standard SCEP protocol, then parameter SCEP_ENTITY_CLASS must be removed.
SCEP_ENTITY_CLASS	String	Null	Specifies to use the enhanced SCEP enrollment request. The value of entity-class is set in SMGR.

VLAN

Configure the following VLAN parameters.

Parameter	Set to	Notes
VLANSEP	0, 1	Specifies VLAN separation.
L2Q	0, 1, or 2	Specifies 802.1Q tagging mode. Assign one of the values: • Auto (0): The deskphone sends tagged packets on L2QVLAN. If DHCP server is unreachable, the dekphone sends untagged packets till VLANTEST time. • Tag (1): The deskphone sends tagged packets on L2QVLAN. If DHCP server is unreachable, the deskphone sends tagged packets with VLAN=0 till VLANTEST time. • Untag (2): The deskphones sends untagged packets.
PHY2VLAN	Non-zero value	This is the data VLAN. The parameter must not have the same value as the L2QVLAN parameter.
L2QVLAN	Non-zero value	This is the voice VLAN. The parameter must not have the same value as the PHY2VLAN parameter.

For the above VLAN configuration, there will be a full VLAN separation between the device and computer packets. The device tries to obtain an IP address from the DHCP server on the voice VLAN. If the device gets an IP address, the device sends all the tagged packets on the voice LAN. Set the PHY2VLAN parameter to the data VLAN so that untagged packets from the computer are

assigned to the data VLAN or the tagged packets from the computer are forwarded to the data VLAN. Tagged packets from computers on VLANs other than the data VLAN are blocked.

FIPS mode

The Federal Information Processing Standard, or FIPS 140-2, is a computer security standard for cryptographic modules used by the U.S. government. FIPS 140-2 specifies the security requirement that a cryptographic module must meet to protect the classified or sensitive data.

OpenSSL libraries include a set of cryptographic algorithms compliant with FIPS 140-2, which is invoked when the library is initiated in FIPS mode. You can enable the FIPS mode using the FIPS_ENABLED parameter that controls the usage of OpenSSL FIPS-certified cryptographic modules. You can set the parameter through the `46xxsettings.txt` file or DHCP option 242.

Note:

In FIPS mode, the CONFIG_SERVER_SECURE_MODE parameter value should be set to 1 ensuring only HTTPS is used to access the configuration server.

Disable the following features when enabling the FIPS mode on the phone:

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

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

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

- **Reboot**: The phone reboots.

Note:

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

Related links

FIPS mode parameter on page 55

FIPS mode parameter

You can set the following parameter in the `46xxsettings.txt` file

Parameter name	Default Value	Description
FIPS_ENABLED	0	This parameter is used for enabling FIPS mode on the phone. Setting the value to 1 specifies only FIPS-approved cryptographic algorithms are supported. Value operation: • 0: No restriction on using non-FIPS approved cryptographic algorithms. • 1: Use only FIPS-approved cryptographic algorithms using embedded FIPS 140-2-validated cryptographic module.

Related links

FIPS mode on page 54

Chapter 5: Phone administration

Introduction

During installation or after you have successfully installed a 9600 Series IP Deskphones, 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 deskphones 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 deskphone until you use the local administrative procedures CLEAR or 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.

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. Enter the administrator password on the Enter access code screen.
2. Select **Enter**.

The Avaya Menu administration file

The Avaya Menu administration file contains parameters to customize Avaya Menu and to view Web links on Avaya Menu. You can administer up to nine Web links.

To customize Avaya Menu, you need to:

- Create the Avaya Menu Administration file named AvayaMenuAdmin.txt and configure appropriate parameters.
- Set the AMADMIN parameter in the settings file to point to the HTTP server location where you save the AvayaMenuAdmin.txt file.

The AvayaMenuAdmin.txt file contains the following parameters:

Parameter	Description
AMTYPExx	Specifies the type of Avaya Menu option that you want to configure. For the 9608, 9608G, and 9611G deskphones, you can assign the following values to this parameter: • 1 for Web link • 2 for the Options & Settings option • 3 for the Network Information option • 4 for the About Avaya one-X option • 5 for the Log Out option For the 9621G and 9641G deskphones, you can assign the following values to this parameter: • 1 for Web link • 2 for the Options & Settings option • 3 for the Network Information option • 4 for the Light Off option • 5 for the Touch Screen Cleaning option • 6 for the About Avaya one-X option • 7 for the Log Out option where, xx is a two-digit integer from 01 to 12. If AMTYPE*xx* is 1 then you must also define the following parameters: • AMLBLxx • AMDATAxx where, xx must be the same for each of the three parameters. If AMTYPExx is 2, 3, or 4, the system ignores any value that you specify for AMLBLxx or AMDATAxx.
AMLBLxx	Specifies the label that the deskphone displays for the Web link. The label must not exceed 16 UTF-16 characters.
AMDATAxx	Specifies the URI for the Web link. The URI must not exceed 255 ASCII characters
AMICONxx	Specifies the icon for the WML applications on the Home screen for the 9621G and 9641G deskphones.

You can specify 12 Web links, but the deskphone displays only the first nine Web links. If you have also configured the browser, the deskphone displays nine Web links that includes the browser.

The deskphone displays any built-in application for which you set the respective parameter to display the application, even if you do not configure that application in the AvayaMenuAdmin.txt file.

Example

```
############################################################
## AVAYA MENU CONFIGURATION FILE TEMPLATE ##
############################################################
## This file is to be used as a template for configuring Avaya Main
## Menu. See the LAN Administrators Guide nd the Avaya one-X™ Deskphone
## Edition for 9600 Series and the Avaya one-X™ Deskphone Edition for
## 9600 Series and the Avaya one-X™ Deskphone Edition for 9600 Series
## IP Telephones Administrator Guide for details.
## Both are available on support.avaya.com
############################################################

## AMLBLxx=Lable up to 16 unicode character
##
## AMTYPExx=Type 1=WML-Application, 2=local Phone Settings,
## 3=local LogOff Application, 4=local About Avaya Screen,
## 5=Guest Login Application, 6=Digital Screensaver
##
## AMDATAxx        URI of up to 255 ASCII-characters
## e.g. http://yy.yy.yy.yy/*.wml
##
## The tags AMLBLxx and AMDATAxx are only used if AMTYPExx = 1
## AMICONxx is used to set icons for WML Applications on Home Screen.
## AMICONxx is only used if AMTYPExx = 1.
##
## Multiple definitions of local applications (Type 2..4)
## will be supressed. The last tag is valid.
##
## xx describes the sequence in A-Menu and is valid
## from 01 to 12
##

##AMTYPE01=
##AMLBL01=
##AMDATA01=
##AMICON01=

##AMTYPE02=
##AMLBL02=
##AMDATA02=
##AMICON02=

##AMTYPE03=
##AMLBL03=
##AMDATA03=
##AMICON03=

##AMTYPE04=
##AMLBL04=
##AMDATA04=
##AMICON04=

##AMTYPE05=
##AMLBL05=
##AMDATA05=
##AMICON05=
```

```
##AMTYPE06=
##AMLBL06=
##AMDATA06=
##AMICON06=

##AMTYPE07=
##AMLBL07=
##AMDATA07=
##AMICON07=

##AMTYPE08=
##AMLBL08=
##AMDATA08=
##AMICON08

##AMTYPE09=
##AMLBL09=
##AMDATA09=
##AMICON09=

##AMTYPE10=
##AMLBL10=
##AMDATA10=
##AMICON10=

##AMTYPE11=
##AMLBL11=
##AMDATA11=
##AMICON11=

##AMTYPE12=
##AMLBL12=
##AMDATA12=
##AMICON12=
```

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.
- CALIBRATION - Applicable to 9621G and 9641G deskphones. To calibrate the touch screen.
- CLEAR - To remove all administered values, user-specified data, option settings, etc. and return a deskphone 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 CLEAR 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.

Setting the signaling protocol identifier

About this task

Use the following procedure to set or change the Signaling Protocol Identifier when your environment has more than one protocol on a subnet. A valid SIG Protocol Identifier is either **0** (default), **1** (H.323), or **2** (SIP).

Note:

Perform this procedure only if the LAN Administrator instructs you to do so.

Procedure

1. Use the Craft password to gain access to the Administration procedures screen. The default password is **27238**.
2. When you select **SIG...** from the Administration procedures screen, the deskphone prompts you to use the Right and Left navigation arrows to select a setting and displays the following text:

   Setting: *text string* **Choice Selector** where the ***text string*** is the wording associated with the current system value of SIG, defined as:

   - "Default" when SIG = 0
   - "H.323" when SIG = 1

- "SIP" when SIG = 2

Note:

The SIG value "Default" can represent either SIP or H.323 depending on the upgrade file used for the deskphone.

3. To change the setting, press the **Change** softkey until you see the setting you want or use the **Right** or **Left** navigation arrow to cycle through the settings.

   Depending on the current value, the next sequential text string is selected and displayed as the setting. For example, if the current value is SIP (2), pressing the Right arrow changes the value to 0 (default). If the current value is H.323 (1), pressing Right arrow changes the value to 2 (SIP).

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

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

Configuring SIP settings

About this task

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

Procedure

1. Select **SIP** from the Administration procedures screen.

   The phone displays the following:

   - **SIP Global Settings**
   - **SIP Proxy Server**

2. Press **Select** or **OK** or the corresponding line button to change any of the following SIP global settings:

   - **SIP Domain**: Changes the domain parameter of SIP.
   - **Avaya Environment**: Specifies whether the available SIP Avaya environment is in effect.

     The two modes to detect the available environment are as follows:

     - **Auto**: Detects the Avaya environment automatically.
     - **No**: Does not detect the Avaya environment and switches to a non-Aura mode.

   - **Reg Policy**: Specifies the registration policy for SIP.

     The two modes are as follows:

     - **alternate**: Supports registration to one of the active controllers.

- **simultaneous**: Supports registration to more than one active controllers.

- **Failback Policy**: Specifies the fail back policy.

  The two modes are as follows:

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

- **Proxy Policy**: Specifies whether the settings of SIP proxy servers are taken from the `46xxsettings.txt` file or can be edited by the user.

  The two modes are as follows:

  - **Auto**: The settings are taken from the `46xxsettings.txt` file. The user can only view the settings.
  - **Manual**: The user can edit, delete, or create new server properties.

- **Avaya Config Server**: Specifies the IP address of Avaya configuration server, only if PPM is not on the same server as the SIP Proxy server.
- **User ID**: Specifies the user ID of the currently logged in user.
- **Host to Ping:** Checks the host server for response using IP address or DNS.

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 remove the settings or use the **CLEAR** option from the Administration menu on phone.

3. Select **SIP Proxy Server** to change SIP proxy server settings.

   The phone displays a list of currently configured servers.

   Caution:

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

4. Do one of the following:

   - To add a new server, select **New**, enter the following values and select **Save**.

     - **SIP Proxy Server**: Specifies the IP address or DNS for Session Manager deployments. The corresponding parameters are SIP_CONTROLLER_LIST for IPv4 and SIP_CONTROLLER_LIST2 for IPv6 or dual mode.
     - **Transport Type**: Specifies the type of transport. The available options are TCP, UDP, or TLS. The corresponding parameter is SIPSIGNAL.
     - **SIP Port**: Specifies the SIP port. If no value is entered, default of 5060 for UDP/TCP or 5061 for TLS is used. If Transport Type is UDP/ TCP, SIP_PORT_ SECURE is used.

   - To edit a SIP proxy server settings, select the server from the list of configured servers and edit fields such as, **SIP Proxy Server**, **Transport Type**, or **SIP Port**. Select **Save**.

- To delete a SIP proxy server, select **Delete**.

Configuring Time Server settings

About this task

Use this procedure to designate a server for Simple Network Time Protocol (SNTP) and to set corresponding values.

Procedure

1. Use the Craft password to gain access to the Administration procedures screen. The default password is **27238**.
2. When you select **SNTP...** from the Administration procedures screen, the deskphone displays the following settings and prompts you to enter the IP Address of the SNTP server:
   - SNTP Server: Specifies the IP address or DNS of the network time server and changes SNTPSRVR or SNTPSRVR_IN_USE parameters.
   - SNTP GMT offset: Specifies the local time difference in hours from Greenwich Mean Time. The corresponding parameter is GMTOFFSET .
   - SNTP Daylight Savings Time Off/On/Auto: Specifies whether the deskphone should recognize Daylight Savings Time (DST) (0=no DST, 1=DST activated as per DSTOFFSET, 2=automatic based on DSTSTART and DSTSTOP values. The corresponding parameter is DAYLIGHT_SAVING_ SETTING_MODE.
3. Press **Save** to store the new setting and returns to the Administration procedures screen.

Setting the date and time on SIP deskphones

9600 Series IP Deskphones need a source of date and time information. This information typically comes from a network time server running the Simple Network Time Protocol (SNTP). The deskphones use several administrative parameters for this functionality. The parameter SNTPSRVR defines the server's IP Address(es). GMTOFFSET defines the offset from Greenwich Mean Time (GMT). DSTSTART and DSTSTOP define the start and end of Daylight Savings Time, respectively. DSTOFFSET defines the Daylight Savings Time offset from Standard Time. Finally, DATETIMEFORMAT defines the format of the date and time display.

About DNS addressing

support DNS addresses, dotted decimal addresses, and colon-hex 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, non-zero, dotted decimal address. Otherwise DNS fails. The text string for the DOMAIN system parameter, Option 15 is appended to the addresses in Option 6 before the phone attempts DNS address resolution. If Option 6 contains a list of DNS addresses, those addresses are queried in the order given if no response is received from previous addresses on the list. As an alternative to administering DNS by DHCP, you can specify the DNS server and or the domain name in the HTTP script file. But first SET the DNSSRVR and DOMAIN values so that you can use those names later in the script.

Note:

Administer Options 6 and 15 with DNS servers and domain names respectively.

Virtual LAN overview

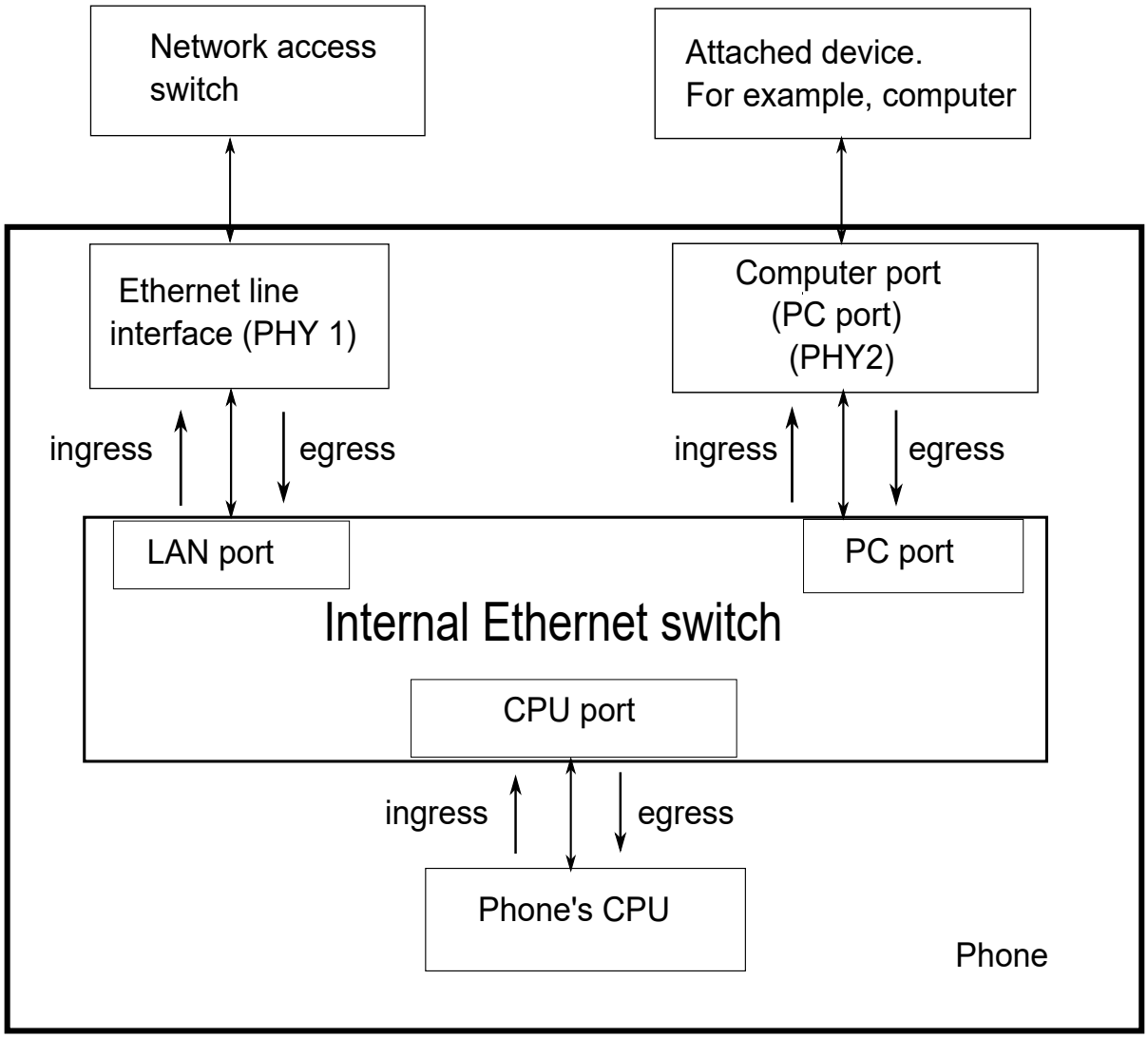
Virtual LANs (VLANs) are used to segregate your network into groups or domains. They can also prioritize the network traffic into each domain. For example, a network can have a Voice VLAN and a Data VLAN. This functionality of grouping devices that have a set of common requirements can simplify network 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 the 802.1Q protocol and the way in which an additional four-byte VLAN tag is inserted at the beginning of an Ethernet frame. This additional VLAN tag describes the VLAN ID to which a particular device belongs and the priority of the VLAN tagged frame. Voice and video traffic get a higher priority in the network because they are subject to degradation caused by network jitter and delay.

VLAN separation

A phone has an internal network switch that can use VLANs to segregate traffic going to 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. Also, you can configure the switch to separate the traffic moving towards the CPU of the phone from the traffic moving towards the PC port.

You can configure the internal switch of the phone by using the `46xxsettings.txt` file, LLDP, or DHCP. However, you must configure the VLAN settings on the internal switch of the phone only through DHCP or LLDP because these protocols are run before and during network initialization. If that is not possible, then use the `46xxsettings.txt` file configuration parameters and start the VLAN in automatic mode, which is the default mode.


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

VLAN separation modes in 9600 Series IP Deskphones

9600 Series IP Deskphones support three VLAN separation modes:

- No VLAN separation mode: The CPU port of the phone receives untagged and tagged VLAN frames on any VLAN irrespective of whether the phone sends untagged or frames. This traffic is received from the PC port or the LAN port. The CPU filters the frames. To reduce unnecessary traffic to the CPU, you must configure only the necessary VLANs on the external switch port, in particular, voice VLAN and data VLAN. To configure the phone to work in this mode, set VLANSEP=0.
- Partial VLAN separation mode: This is the default mode. In this mode, the CPU port sends tagged packets to voice VLAN only. The CPU port receives tagged packets on voice VLAN or untagged packets from LAN port. PC and LAN port can send any traffic between them. To configure the phone to work in this mode, ensure the following conditions :
  - VLANSEP = 1
  - VLANSEPMODE = 0
  - L2Q = 0 (auto) or 1 (tag)
  - VLANTEST = 0 or timer is less than VLANTEST
  - PHY2VLAN = 0
- Full VLAN separation 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 the CPU port and the PC port. To configure the phone to work in this mode, ensure the following conditions:
  - VLANSEP = 1
  - VLANSEPMODE = 1
  - L2Q = 0 (auto) or 1 (tag)
  - L2QVLAN is not equal to 0
  - PHY2VLAN is not equal to 0
  - L2QVLAN is not equal to PHY2VLAN

The DHCP server on voice VLAN is reachable and the phone receives the IP address on voice VLAN when the phone sends tagged VLAN frames.

Configuring an external switch port

About this task

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

Procedure

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

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

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

Exceptions to the VLAN forwarding rules

Exceptions to the VLAN forwarding rules are as follows:

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

Special considerations

Special use of VLAN ID=0

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

Automatic failback of VLAN tagging

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

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

VLAN support on the computer or PC port

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

VLAN parameters

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

Parameter name	Default value	Description
L2Q	0	Specifies whether the VLAN tagging is enabled or disabled. The options are: • 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 the value pair in a DHCPACK message • A SET command in the `46xxsettings.txt` file • DHCP option 43 • LLDP

Table continues…

Parameter name	Default value	Description
VLANTEST	60	Specifies the number of seconds that the phone waits prior to failing back to a different VLAN ID if no response is received from the DHCP server. Valid values are from 0 to 999. The option is: • 0: The phone continues to attempt a DHCP REQUEST forever. VLANTEST is configured through: • `46xxsettings.txt` file • A name equal to the value pair in the DHCPACK message
VLANSEP	1	Specifies whether VLAN separation is enabled by the built-in Ethernet switch while the phone tags frames with a non-zero VLAN ID. The options are: • 0: Disabled • 1: Enabled if L2Q, L2QVLAN, and PHY2VLAN are set appropriately VLANSEP is configured through the `46xxsettings.txt` file.
VLANSEPMODE	1	Specifies whether full VLAN separation is enabled by the built-in Ethernet switch while the phone tags frames with a non-zero VLAN ID. The options are: • 0: Disabled • 1: Enabled PHY2PRIO is not supported when VLANSEPMODE is 1. VLANSEPMODE is configured through the `46xxsettings.txt` file.

Table continues…

Parameter name	Default value	Description
PHY2TAGS	0	Determines whether VLAN tags are stripped on Ethernet frames going out of the computer (PC) port. The options are: • 0: Strips VLAN tags from Ethernet frames leaving the computer (PC) port of the phone. • 1: Does not strip VLAN tags from Ethernet frames leaving the Computer (PC) port of the phone. PHY2TAGS is configured through the `46xxsettings.txt` file.
L2QVLAN	0	Specifies the voice VLAN ID to be used by IP phones. Valid values are from 0 to 4094. L2QVLAN is configured through: • A local admin procedure • A name equal to the value pair in the DHCPACK message • A SET command in the `46xxsettings.txt` 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 from 0 to 4094. PHY2VLAN is configured through: • A SET command in the `46xxsettings.txt` file • LLDP

Table continues…

Parameter name	Default value	Description
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, for example, RTP, RTCP, SRTP, and SRTCP. All other frames, except those specified by the L2QSIG parameter, are set to priority 0. Valid values are from 0 to 7. L2QAUD is configured through: • A SET command in the `46xxsettings.txt` 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, for example, SIP. All other frames, except those specified by the L2QAUD parameter, are set to priority 0. Valid values are from 0 to 7. L2QSIG is configured through: • A SET command in the `46xxsettings.txt` file • LLDP
PHY2PRIO	0	Specifies the layer 2 priority value to be used for frames received on the secondary Ethernet interface when VLAN separation is enabled. Valid values are from 0 to 7. PHY2PRIO is configured through the `46xxsettings.txt` file.

IEEE 802.1X overview

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

You must configure the following parameters for this feature:

Parameter name	Default value	Description
DOT1XSTAT	0	Specifies the 802.1X Supplicant operating mode. Values: • 0: Supplicant disabled. • 1: Supplicant enabled, but responds only to received unicast EAPOL messages. • 2: Supplicant enabled and responds to received unicast and multicast EAPOL messages. You can configure the parameter using the following sources: • Admin menu • `46xxsettings.txt` file
DOT1X	0	Specifies the 802.1X pass-through operating mode. Using this parameter, a phone can pass through 802.1X traffic to and from the PC port and send an EAP-logoff to the network using the MAC address of the device that gets removed from the PC port. Values: • 0: EAPOL multicast pass-through enabled without proxy logoff. • 1: EAPOL multicast pass-through enabled with proxy logoff. • 2: EAPOL multicast pass-through disabled. You can configure the parameter using the following sources: • Admin menu • `46xxsettings.txt` file
DOT1XEAPS	MD5	Specifies the authentication method to be used by 802.1X. Values: • MD5: 802.1X supplicant uses EAP-MD5 authentication. • TLS: 802.1X supplicant uses EAP-TLS authentication.

Setting the 802.1x operational mode

About this task

Use the following procedure to set or change the 802.1x operational mode for secure layer 2 network access.

Before you begin

Set the DOT1X configuration parameter to "0" or "1" for the deskphone to support 802.1X pass-through and the DOT1XSTAT configuration parameter to "1" or "2" for the deskphone to support supplicant operation.

Procedure

1. Use the local procedure (Craft) to go to the Admin menu.
2. Scroll to **802.1X**.

   The following parameters are listed:

   - DOT1X (802.1X Pass-Thru Mode)
   - DOT1XSTAT (802.1X Supplicant Mode)

   The two settings represent the text strings associated with the current configuration parameter values of DOT1X (802.1X Pass-Thru Mode) and DOT1XSTAT (802.1X Supplicant Mode)
3. Select the option you want to change and press the **Change** softkey.
   - For the Pass-thru mode:
     - "On" if DOT1X = 0
     - "On & proxy logoff" if DOT1X = 1
     - "Off" if DOT1X = 2
   - For the Supplicant:
     - "Off" if DOT1XSTAT = 0
     - "On" if DOT1XSTAT = 1
     - "On with multicast" if DOT1XSTAT = 2
4. Press **Save**.

   The deskphone restarts if you make any change to the 802.1X data.

Setting Site-Specific Option Number

About this task

Use this procedure to set the Site-Specific Option Number (SSON) for the phone.

Caution:

Do not perform this procedure if you are using static addressing. Set SSON for the phones only if you are using DHCP and your LAN administrator instructs you to set SSON.

Procedure

1. Use the Craft password to go to the Admin menu.
2. Scroll to **SSON** and press OK.

   The phone displays the current value of DHCP_SSON under Setting.
3. To change the SSON value, enter a value between 128 and 254.
4. Press **Save** to store the new setting and return to the Administration procedures screen.

Setting the group identifier

About this task

Use the following procedure to set or change the group identifier settings for the phones. You can also set this value using System Manager and Personal Profile Manager (PPM).

Note:

Perform this procedure only if the LAN administrator instructs you to do so.

Procedure

1. Use the Craft password to go to the Admin menu..
2. Scroll to **GROUP**.
3. Enter a valid **Group** value between 0-999.
4. Press **Save**.

   The phone restarts to apply the new settings.

GROUP parameter for customized user groups

Your communication setup might have different users who use the same phone models but require different configuration settings. For example, user groups have different time zones or work activities.

You can use the GROUP parameter for the following purposes:

- Identify which deskphones are associated with which group and designate a number for each group. The Group number can be any integer from 0 to 999. The default value of the

parameter is 0. If you select the default value, the phone assigns the largest deskphones group as Group 0.

- At each non-default deskphone, instruct the installer or the user to invoke the GROUP from the CRAFT menu and specify which GROUP number to use. The installer or the user can set the GROUP System value on a deskphone-by-deskphone basis.

  For more information about using the CRAFT menu to set a GROUP value, see Setting the group identifier on page 76.

- When the GROUP assignments are in place, edit the settings file to allow each deskphone of the appropriate group to download its proper settings.

Example

The following is an example of a settings file with deskphones in three different groups- group "0" (the default), group "1", and group "2":

```
## First check if this phone is in group 1.
## If it is, jump to the tag GROUP1
##
IF $GROUP SEQ 1 goto GROUP1
##
## Now check if this phone is in group 2.
## If it is, jump to the tag GROUP2
IF $GROUP SEQ 2 goto GROUP2
##
## The phone is not in either GROUP 1 or 2 so it is in GROUP 0
## {specify settings unique to Group 0}
GOTO END
# GROUP1
## GROUP 1-only settings go here
## {specify settings unique to Group 1}
GOTO END
# GROUP2
## GROUP 2-only settings go here
## {specify settings unique to Group 2}
# END
## The settings here apply to all three groups
## {specify settings common to all Groups}
```

Example

Note:

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

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

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

Using the VIEW administrative option

About this task

Use the following procedure to verify the current values of system parameters and file versions.

Note:

Users can view but not change the Craft parameters.

Procedure

1. Use the Craft password to go to the Admin menu..
2. Scroll to **VIEW** to view the parameter details.
3. Press **Back** to return to the Admin menu.

VIEW field description

Setting	Description	Associated Configuration Parameter
Model	The model of the phone that is set by factory procedures.	MODEL
Application File	The name of the Signed Application/Library software package.	
Boot File	The name of the boot file.	
FIPS	The FIPS mode is displayed.	FIPS_ENABLED
Protocol	Signaling protocol in effect, such as SIP.	
Group	The group identifier to download during start-up a specific configuration set for a dedicated user group.	GROUP
MAC	The MAC address of the phone.	MACADDR
SIP Proxy Server	The SIP proxy server to which the phone registered successfully.	SIPPROXYSRVR_IN_ USE
Presence Server	The IP address of the presence server.	
Gateway	The primary gateway out of the list of configured ones.	ROUTER_IN_USE
HTTPS Server	The list of IP or DNS addresses of TLS servers for HTTPS file download, settings file or language files, during start-up procedure.	TLSSRVR

Table continues…

Setting	Description	Associated Configuration Parameter
HTTP Server	The list of IP or DNS addresses of HTTP servers for HTTP file download, settings file or language files, during startup procedure.	HTTPSRVR
DNS Server	The IP address of the DNS server that the phone accessed before successfully.	DNSSRVR_IN_USE
SNTP Server	The SNTP server that the phone used before to set or update the date and time.	SNTPSRVR_IN_USE
Product ID	The device ID of the phone.	
Phone SN	Phone Serial Number	
Exchange Server	The Microsoft Exchange™ server that the phone uses currently.	EXCHANGE_ SERVER_IN_USE

Push server

The Push feature requires a trusted push server. The push server administration must conform to the requirements in *9600 Series IP Telephone Application Programmer Interface (API) Guide*.

Related links

Secure Push on page 79

Secure Push

Secure Push allows the data transmission to the trusted applications. It is done using a secured connection for sending their content to the 96x1 series IP Deskphones without any action required from the user.

Secure Push is similar to non-secure except that the secure Push uses HTTPS for incoming and outgoing requests to the phone. The URI of the secure Push uses DNS name instead of the IP address for hostname validation.

The initial `subscribe` message sent to the server indicates if secure or non-secure Push is supported by phone.

The administrator should enable the PUSH_MODE parameters in the settings file to provide the combination of secure and non-secure Push connections.

Note:

It is mandatory to install the Push Servers Identity certification in the phone for secure Push connection. If no Identity certificate is installed, `push mode` is ignored and only HTTP is used.

Related links

Push server on page 79

SNMP activation

9600 Series IP Deskphones is compatible with SNMPv2c and SMIv2. The deskphones respond correctly to queries from entities that comply with earlier versions of SNMP, such as SNMPv1. The deskphones respond to queries directed either at the MIB-II or the read-only Custom MIB. Read-only means that the values therein cannot be changed externally by means of network management tools.

You can restrict the IP addresses from which the deskphone accepts SNMP queries with the SNMPADD parameter. You can also customize your community string with the SNMPSTRING parameter. For more information, see Chapter 5: Administering DHCP and HTTP servers .

SNMP is disabled by default. Administrators must initiate SNMP by setting the SNMPADD and SNMPSTRING parameters appropriately.

For more information about SNMP and MIBs, see the IETF website: http://www.ietf.org. The Avaya Custom MIB for the 9600 Series IP Deskphones is available for download in *.txt format on the Avaya support website: http://support.avaya.com.

Registration and authentication

9600 Series IP Deskphones require an outbound proxy SIP (OPS) extension on Communication Manager and a login and password on Session Manager to register and authenticate.

For the SIP Deskphones to work properly, you must specify the correct domain name on the IP Network Region screen of Communication Manager.

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

- For information about the IP Network Region screen, see *Administering Network Connectivity on Avaya Aura® Communication Manager* at the Avaya Support website: http://support.avaya.com.
- For information about the registration process, see *Maintaining Avaya Aura® Session Manager* and *Troubleshooting Avaya Aura® Session Manager*. Also, see your call server administration documentation.

IP address and settings reuse

After a successful registration with a call server, the IP address of the deskphone and the parameter values are saved in the non-volatile memory of the deskphone. The deskphone can reuse the saved parameters if the DHCP or HTTP/HTTPS server is not available for any reason after the deskphone restarts.

IP Address reuse was added to prevent infinite looping when separate DHCP servers are used for voice and data VLANs, and a response is received from the DHCP server on the data VLAN, but not on the voice VLAN.

Unless indicated otherwise, the values described here during IP address reuse are internally provisioned or set by the process itself and not by manual administration.

- Routers in Use - if no responses are received from the routers indicated in the configuration parameter ROUTER (set using DHCP Option 3 or by a local administrative procedure), and if REUSE = 1, then ROUTER_IN_USE will be set to REUSE_ROUTER_IN_USE. With the exception of the ROUTER configuration parameter, the other router-related parameters are internally set system values.
- VLAN Check - During the VLAN check, if a reset is to be done and VLAN_IN_USE is not zero, VLAN_IN_USE will be added to VLANLIST if it is not already on VLANLIST.

  The VLAN detection process described in Automatically detecting a VLAN on page 52 is followed if tagging is off or if tagging is on and L2QVLAN is > 0, and if REUSETIME > 0, and if REUSE_IPADD is not “0.0.0.0”. If VLANTEST expires, the value of VLAN_IN_USE is added to VLANLIST if it is not already on VLANLIST.

If a DHCPOFFER is not received within REUSETIME seconds, or if a DHCPOFFER is received that contains a value of L2QVLAN that is on VLANLIST, REUSE will be set to 1, IPADD will be set to the value of REUSE_IPADD, NETMASK will be set to the value of REUSE_NETMASK, ROUTER will be set to the value of REUSE_ROUTERS, and if the value of REUSE_TAGGING is 1, 802.1Q tagging will be turned on with a VLAN ID equal to the value of L2QVLAN_INIT, DHCP will then enter the “extended” REBINDING state, and operation will proceed as normal.

After a successful registration, the following system values are set:

- REUSE_IPADD will be set to the value of IPADD
- REUSE_NETMASK will be set to the value of NETMASK
- REUSE_ROUTERS will be set to the value of ROUTER
- REUSE_ROUTER_IN_USE will be set to the value of ROUTER_IN_USE
- REUSE_TAGGING will be set to the value of TAGGING
- L2QVLAN_INIT will be set to the value of VLAN_IN_USE
- The MIB object endptVLANLIST will be set to the value of VLANLIST and then the value of VLANLIST will be set to null.

Ping and traceroute

All 9600 Series IP Deskphones respond to a ping or traceroute message sent from the call server switch or any other network source.

For more information, see your call server administration documentation.

TCP and UDP ports

9600 Series IP Deskphones use different protocols, such as TCP, TLS, and UDP to communicate with other equipment in the network. Part of this communication identifies which TCP or UDP ports each piece of equipment uses to support each protocol and each task within the protocol. Depending on your network, you need to know what ports or ranges are used in the operation of the phones.

Received packets (destination = SIP phone)

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

Table continues…

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

Transmitted packets (source = SIP phone)

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

Table continues…

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

Preinstallation checklist for static addressing

Before performing static addressing, verify all the network requirements first. In addition, you must have the values for the following parameters:

- IP address of the deskphone.
- IP address of the router.
- IP subnet mask.
- IP address of the HTTP and/or HTTPS server (applicable for only DHCP server settings).
- IP address of the DNS Server.
- VLAN ID (the L2QVLAN value).

- VLANTEST value.

Assigning static IP address

Use static IP addressing, if the setup does not require a DHCP server.

Procedure

1. In the Administration menu, go to **ADDR**.
2. In the **IP Address** field, enter the IP address. For the description of other fields, see Static addressing field descriptions.
3. Use the navigation arrows to scroll to and highlight the address you want to change. Choose one of the following options:

Option	Description
IP Address	IP addresses have four sets of three digits followed by a period. Pressing ***** followed by three digits causes a period to be placed in the next position, and the cursor to advance one position to the right.
VLAN ID	Use the dialpad to enter the new static VLAN ID of from 0 to 4094, inclusive.
VLANTEST	Use the dialpad to enter the new value of the DHCPOFFER wait period of from 0 to 999, inclusive.
Host to Ping	Use the dialpad to enter the host server IP address or the DNS name of the server you want to check. The deskphone sends four pings and displays the results in a text block screen. If the ping fails, the following message is displayed. `Unable to contact host`

4. Do one of the following:
   - Press **Save** to store the new setting.
   - Press **Cancel** to return to the Administration menu.
   - Press **OK** after setting ping to the host server and return to the Static Address screen.

   Once the new values are stored, the deskphone is reset. If a new boot program is downloaded from the HTTP/HTTPS server after you enter static addressing information, you must reenter your static addressing information.

Static addressing field descriptions

Configuration Parameter Name	Description
Use DHCP	Choose one of the following options: • **Yes**: Selects the DHCP option. • **No**: Deselects the DHCP option.
Phone	Specifies the IP address of the deskphone. The available format is ***nnn.nnn.nnn.nnn***
Router	Specifies the router IP address. The available format is ***nnn.nnn.nnn.nnn***
Mask	Specifies the network mask. The available format is ***nnn.nnn.nnn.nnn***
HTTPS File Server	Specifies the IP address of the HTTPS file server. The available format is ***nnn.nnn.nnn.nnn***
HTTP File Server	Specifies the IP address of the HTTP file server. The available format is ***nnn.nnn.nnn.nnn***
DNS Server	Specifies the IP address of the DNS server. The available format is ***nnn.nnn.nnn.nnn***
802.1Q	Choose one of the following options: • **0**: Automatic mode. • **1**: Turns on the configuration. • **2**: Turns off the configuration.
VLAN ID	Specifies the ID for VLAN. The available format is ***dddd***.
VLAN TEST	Specifies the duration to wait for the DHCP in seconds. The available format is ***ddd***.

Table continues…

Configuration Parameter Name	Description
Host to ping	Specifies the IP address or the DNS name. The available format are: • ***nnn.nnn.nnn.nnn*** : For IP address. • ***AVohhhhhh*** : For DNS name. ***hhhhhh*** are ASCII characters for the hexadecimal representation of the last three octets of the deskphone's MAC address ***o*** has one of the following values: - “A” if the OID is 00-04-0D - "B" if the OID is 00-1B-4F - "E" if the OID is 00-09-6E - "L" if the OID is 00-60-1D - "T" if the OID is 00-07-3B - "X" if the OID is anything else

Administering display language options

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

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

- Arabic
- Dutch
- English
- French (Canada)
- French (France)
- German
- Hebrew
- Italian
- Japanese
- Korean
- Polish
- Portuguese (Brazil)
- Russian
- Simplified Chinese

- Spanish (Latin America)
- Spanish (Spain)
- Thai
- Traditional Chinese
- Turkish

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

Note:

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

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

For better readability, the phone can display the English fonts in a bigger font-size. For information on how to administer this feature, see Setting a larger display font size. The downloadable language files contain all the information required for the phone to present the language as part of the user interface.

Use the configuration file (46xxsettings.txt) and the following parameters to customize the settings for up to four languages

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

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

Network audio quality

Users can view icons on the deskphone that provide information about:

- Audio quality of a call. A Local Network Quality (LNQ) icon appears whenever the audio quality of a call is below a certain threshold. You can define the threshold in the settings file using the LNQ and QLEVEL_MIN parameters. LNQ is based on a combination of jitter, packet loss, and delay.

- Use of the wide band codec. The HD icon appears if the deskphone uses the wide band codec. You can enable or disable the icon based on the value you assign to the WBCSTAT parameter in the settings file.

For more information about the settings file parameters, see Customizable system parameters for SIP-based 9600 Series IP Deskphones on page 2.

Users can also monitor the network audio performance on a call. The Network Information screen displays the audio network. Users can gain access to the Network Information screen from the Avaya menu. On a touchscreen deskphone, users can gain access to the Network Information screen from the Home screen.

The implication for LAN administration depends on the values the user reports and the specific nature of your LAN, like topology, loading, and QoS administration. This information gives the user an idea of how network conditions affect the audio quality of the current call. Avaya assumes you have more detailed tools available for LAN troubleshooting.

Network progress tones overview

The SIP-based 9600 Series IP Deskphones provide country-specific network progress tones which are presented to the user at appropriate times. The tones are controlled by administering the COUNTRY parameter for the country in which the deskphone will operate. Each Network Progress Tone has the following six components:

- Dialtone
- Ringback
- Busy
- Congestion
- Intercept
- Public Dialtone

All countries listed in this appendix are applicable to the 96xx phones. Some of the dialtone entries have changed from previous releases to be distinctively different than the public dialtone entries.

Alphabetical country list

A:

- Abu Dhabi
- Albania
- Argentina
- Australia
- Austria

B:

- Bahrain
- Bangladesh
- Belgium
- Bolivia
- Bosnia
- Botswana
- Brunei
- Bulgaria

C:

- China (PRC)
- Colombia
- Costa Rica
- Croatia
- Cyprus

D:

- Denmark

E:

- Ecuador
- El Salvador
- Egypt

F:

- Finland
- France

G:

- Germany
- Ghana
- Greece
- Guatemala

H:

- Honduras
- Hong Kong

I:

- Iceland

- India
- Indonesia
- Ireland
- Israel

J:

- Japan
- Jordan

K:

- Kazakhstan
- Korea
- Kuwait

L:

- Lebanon
- Liechtenstein
- Luxembourg

M:

- Macedonia
- Malaysia
- Mexico
- Moldova
- Morocco
- Myanmar

N:

- Netherlands
- New Zealand
- Nicaragua
- Nigeria Norway

O:

- Oman

P:

- Pakistan
- Panama
- Paraguay
- Peru

- Philippines
- Poland
- Portugal

Q:

- Qatar

R:

- Romania
- Russia

S:

- Saudi
- Arabia
- Serbia
- Singapore
- Slovakia
- Slovenia
- Spain
- South Africa
- Sri Lanka
- Swaziland
- Sweden
- Switzerland
- Syria

T:

- Taiwan
- Tanzania
- Thailand
- Turkey

U:

- Ukraine
- United Arab Emirates
- United Kingdom
- Urugua
- USA

V:

- Venezuela
- Vietnam

Y:

- Yemen

Z:

- Zimbabwe

Administering enhanced local dialing

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

The following configuration parameters are applicable to this feature:

Parameter name	Default value	Description
ELD_SYSNUM	1	Specifies whether enhanced local dialing algorithm will be applied for system numbers. Value operation: • 0: Disable enhanced local dialing for system numbers. • 1: Enable enhanced local dialing for system numbers.
ENHDIALSTAT	1	Specifies if the algorithm defined by the parameter is used during certain dialing behaviors. Value operation: • 0: Disables algorithm. • 1: Enables algorithm, but not for contacts. • 2: Enables algorithm, including contacts.
PHNCC	1	Specifies the international country code of the Communication Manager call server. For example, 1 for the United States, 44 for the United Kingdom, and so on. Valid values are from 1 to 999.

Table continues…

Parameter name	Default value	Description
PHNDPLENGTH	5	Specifies the internal dial plan number length. For example, if the extension number is 12345, then the dial plan length is 5. This value must match the extension length set on your call server. Valid values are from 3 to 13.
PHNIC	011	Specifies the international access code. Valid values are from 0 to 4 characters such as numbers 0–9, and special symbols such as star key (*), and pound key (#).
PHNLD	1	Specifies long distance access code. Valid values are from 0 through 9 and empty string.
PHNLDLENGTH	10	Specifies the maximum length, in digits, of the national telephone number for the country in which the Communication Manager call server is located. For example, 800-555-1111 has a length of 10. Valid values are from 5 to 15.
PHNOL	9	Specifies the outside line access code. Valid values are from 0 to 2 characters such as numbers 0–9, and special symbols such as star key (*), and pound key (#).

Note:

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

Enhanced Local Dialing scenarios

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

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

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

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

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

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

  Note:

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

Setting the dial plan on SIP deskphones

During manual dialing, a dial plan allows a call to be initiated without using a **Send** button and without waiting for the expiration of a timeout interval. The dial plan consists of one or more format strings. When the dialed digits match a format string in the DIALPLAN configuration parameter, the call is initiated.

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

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

- + = the character following the + can repeat 0 or more additional times, for a valid match

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

Dial plan example:

"[2-4]xxx|[68]xxx|*xx|9Z1xxxxxxxxxx|9z011x+"

where:

- **[2-4]xxx**: Four-digit dial extensions, with valid extensions starting with 2, 3, or 4;
- **[68]xxx**: Four-digit dial extensions, with valid extensions starting with 6 or 8;
- ***xx**: Two-digit Feature Access Codes, preceded by a *;
- **9Z1xxxxxxxxxx**: Network Access Code ("9 for an outside line"), followed by dial tone, followed by any string of 10 digits– typical instance of Automatic Route Selection (ARS) for standard US long distance number;
- **9z011x+:** Network Access Code ("9 for an outside line"), followed by dial tone, followed by at least one digit – typical instance of Automatic Route Selection (ARS) for US access to international numbers of unknown, and variable, length.

Additional parameters that affect dialing are as follows:

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

Example 1 - Setting the parameter configuration:

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

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

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

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

Administering emergency numbers

Set the PHNEMERGNUM configuration parameter in the settings file or in the Session Manager to assign a default emergency number. The phone automatically dials the configured number whenever a user presses the **Emerg** softkey on the Login screen, or the Phone screen, or when the user presses the **Yes** softkey on an Emergency Calling pop-up screen. The phone dials the emergency number even if the phone is locked or the user is not logged in. You must select the **Allow Unauthenticated Emergency Calls** field in System Manager so that users can dial the emergency number when the phone is not registered.

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

Note:

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

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

Administering audio equalization

Part 68 of the Federal Communication Commission (FAC) rules governs the connection concerning Hearing Aid Compatibility (HAC) and volume control for phones. The HAC feature is an alternative way to provide audio equalization on a handset, from the acoustic standards specified in TIA-810/920 and S004, and may be of benefit to some users of t-coil capable hearing aids.

- Settings File: The administrator can set ADMIN_HSEQUAL. The default value, 1, specifies Handset equalization that is optimized for acoustic TIA 810/920 performance unless otherwise superseded by Local Procedure or User Option. The alternate value, 2, specifies HAC.
- Local Procedure: When users are denied access to Options for administrative reasons, but individual users need an equalization value other than the one in the settings file, the HSEQUAL Craft Procedure provides another method to administer the deskphone with the audio equalization value that you require. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**. "Default" uses the settings file value unless superseded by User Option. "Audio Opt." is optimized for TIA-810/920 acoustic performance, and "HAC Opt." is optimized for HAC telecoil performance.
- User Option: The user can select "Default" by which the deskphone uses the settings file value (unless superseded by Local Procedure), "Audio Opt." which uses Handset equalization that is optimized for acoustic TIA 810/920 performance, or "HAC Opt." which uses Handset equalization that is optimized for electrical FCC Part 68 HAC telecoil performance.
- Handset equalization options are effected in the following order:
  - The deskphone uses the User Option value if selected and saved.
  - If a Local Procedure value was selected and saved, the deskphone uses the local procedure value.
  - If a Settings file value is specified and saved the deskphone uses that value.
  - If none of the above options are set, the deskphone uses Handset equalization that is optimized for TIA-810/920 acoustic performance.

Setting the handset audio equalization

About this task

Use the following procedure to configure the Handset Equalization settings:

Procedure

1. On the user menu, navigate to **Settings > Options&Settings > Advanced Options > Handset Equalization**.

2. Using the navigational keys or by tapping the arrow icons on the screen, choose any of the following:
   - Default
   - Audio Opt
   - HAC Opt
3. Press **Save**.

Enabling and disabling Automatic Gain Control

About this task

Use the following procedure to turn automatic gain control for the handset, headset, and the speaker on or off.

Procedure

1. Enter the Administration menu and select **AGC**.
2. Choose one of the following options:
   - Handset AGC: Toggle “On” or “Off” using navigation arrow or **Change** softkey.
   - Headset AGC: Toggle “On” or “Off” using navigation arrow or **Change** softkey.
   - Speaker AGC: Toggle “On” or “Off” using navigation arrow or **Change** softkey.
3. Press **Save** to store the configuration.

Administering headset profiles

The SIP-based 9600 Series IP Deskphones support signaling for headsets that are connected through the analog headset port on the deskphone. Users can make, answer, or disconnect calls through controls on the headset. Users call also control the headset through the buttons available on their deskphone.

Using the headset

- When the deskphone receives a call, the headset produces an audible beep and the user can answer the call by pressing a button on the headset.
- When a call is established, the user can disconnect the call by pressing a button on the headset.
- When a user makes or receives a call using the buttons on the deskphone, the headset automatically connects the speech path without the need for the user to press any buttons on the headset.

Note:

By default, the deskphone displays the name of the headset profiles that Avaya provides. You can use the HEADSET_PROFILE_ NAMES parameter to change the name of the headset profiles.

Calibrating the touch screen

Screen calibration properly aligns the touch screen but should only be used for a significant problem with the touch screen.

Important:

Use a pencil, a pen, or a stylus rather than your finger to touch the calibration points precisely.

Note:

The CLEAR Craft procedure clears any calibration data set using the CALIBRATE SCREEN Craft procedure, but does not affect factory-set calibration data. Use the **Default** softkey to restore factory-set calibration. Calibration results are not saved as part of a backup. The feature is not supported on the 9641GS deskphone.

About this task

Use this procedure to calibrate 9621 and 9641 touch screen phones.

Procedure

1. Enter the Administration menu using the password.
2. Select the **CALIBRATE SCREEN** form the screen.
3. Choose one of the following options:
   - **Cancel**: To returns to the Administration menu screen without calibrating.
   - **Default**: To reset the calibration parameters to the factory default.
   - **Start**: To calibrate the screen.
     - Touch the center of the target with the stylus as soon as it appears.
     - Touch the next target's center with the stylus within 10 seconds of its appearance.
     - Repeat steps to complete all four targets with the following message:`Calibration successful`
4. Press **Save** to save the settings.

Using the Debug Mode

Before you begin

Ensure that the following values are changed:

- Value of PROCPSWD parameter is set to a value other than default. When the ADMIN_PASSWORD is set, then the parameter PROCPSWD is not used.
- Value of SLMCAP parameter is set to “3”.
- Value of SLMCTRL parameter is set to “2”.

Procedure

1. Use the Craft password to gain access to the Administration procedures screen.
2. Navigate to **DEBUG** from the Administration procedures screen. The following debug options are available:

- Debug Mode
- Service mode control
- Service mode record

3. To enable or disable the options, tap or use the appropriate buttons.
4. Press **Save** to store the new setting.

   Restart the deskphone for the DEBUG settings to take effect.

Setting interface control

About this task

Use the following procedure to set or change the interface control value.

Procedure

1. Use the Craft password to gain access to the Administration procedures screen. The default password is **27238**.
2. When you select **INT...** from the Administration procedures screen, the following text displays with a prompt to use the Right and Left navigation arrows to select a setting:

   Ethernet: Choice Selector

   PC Ethernet: Choice Selector

   The values shown are the text strings associated with the current PHY1STAT on the Ethernet line and the current PHY2STAT system value on the PC Ethernet line. The PHY1STAT text strings are:

   - "Auto" when PHY1STAT = 1

- "10Mbps half" when PHY1STAT = 2
- "10Mbps full" when PHY1STAT = 3
- "100Mbps half" when PHY1STAT = 4
- "100Mbps full" when PHY1STAT = 5
- "1000Mbps full" when PHY1STAT = 6

Note:

A PHY1STAT value of 6 applies only to deskphone models that support Gigabit Ethernet (GigE), otherwise this value/choice does not display.

The PHY2STAT text strings are:

- "Disabled" when PHY2STAT = 0
- "Auto" when PHY2STAT = 1
- "10Mbps half" when PHY2STAT = 2
- "10Mbps full" when PHY2STAT = 3
- "100Mbps half" when PHY2STAT = 4
- "100Mbps full" when PHY2STAT = 5
- "1000Mbps full" when PHY2STAT = 6

Note:

A PHY2STAT value of 6 applies only to deskphone models that support Gigabit Ethernet (GigE), otherwise this value/choice does not display.

3. To change the Ethernet setting, press the **Right** navigation arrow or the **Change** softkey to cycle through the possible settings.

   Depending on the current value, the next sequential text string is selected and displayed as the setting. For example, if the current value is 10 Mbps half (2), pressing the Right navigation arrow changes the value to 10 Mbps full (3). If the current value is 1000 Mbps full (6), pressing the Right navigation arrow changes the value to Auto (1).
4. To change the PC Ethernet setting, select that line and press the Right navigation arrow or **Change** to cycle through the possible settings.
5. Press **Save** to store the new setting(s) and redisplay the Admin Procedures screen.

Enabling and disabling event logging

About this task

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

Procedure

1. Use the Craft password to gain access to the Administration procedures screen. The default password is **27238**.
2. When you select **LOG** rom the Administration procedures screen, the deskphone prompts you to use the Right and Left navigation arrows to select and change a setting and displays the following text:

   where the ***text string*** is the wording associated with the current system value of SYSLOG_ENABLED (1 = Enabled; 0 = Disabled) and SYSLOG_LEVEL, defined as:

   - "Emergencies" when SYSLOG_LEVEL = 0
   - "Alerts" when SYSLOG_LEVEL = 1
   - "Critical" when SYSLOG_LEVEL = 2
   - "Errors" when SYSLOG_LEVEL = 3
   - "Warnings" when SYSLOG_LEVEL = 4
   - "Notices" when SYSLOG_LEVEL = 5
   - "Information" when SYSLOG_LEVEL= 6
   - "Debug" when SYSLOG_LEVEL = 7
3. To change the **Log** or **Remote Logging Enabled** setting, press the Right (or Left) navigation arrow to cycle through the valid settings. When changing the Remote Log Server value, enter the IP Address to which syslog messages should be sent.

   When changing the **Log** value, depending on the current value, the next sequential text string or value is selected and displayed as the setting. For example, if the current value is Alerts (1), pressing the Right navigation arrow changes the value to Critical (2). If the current value is Debug (7), pressing the Right navigation arrow changes the value to Emergencies (0).
4. Press **Save** to store the new setting and redisplay the Administration procedures screen.

   Logging has a direct impact on performance. Only turn on the required categories and turn them off as soon as logging is not required.

Long-term acoustic protection

You can enable the long-term acoustic protection feature to protect the ears of the headset user. Long-term acoustic protection is supported only in L100 Series Headsets with RJ9 connector, when the headset profile is set to Profile1. You can configure this feature by using the `46xxsettings.txt` file.

Related links

Long-term acoustic exposure protection parameter on page 104

Long-term acoustic exposure protection parameter

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

Parameter name	Default value	Description
ACOUSTIC_EXPOSURE_PROTECT_MODE_DEFAULT	1	Specifies the acoustic exposure protection mode. The options are: • 1: Off • 2: Dynamic • 3: 4 hours • 4: 8 hours

Related links

Long-term acoustic protection on page 103

No Hold Conference

With the No Hold Conference feature, you can add participants to your call while continuing your active conversation. The No Hold Conference feature lets you create a conference call without putting any call participant on hold.

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

Your administrator can configure your phone to support the no hold conference feature on a button module. You can use the call appearance for a regular or pre-configured number.

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

The administrator can pre-configure only one number on System Manager. When you press the **No Hold Conf** button, the call is placed to the pre-configured number when the participant answers the call joins the no hold conference.

If the participants do not answer the call within the configured time-out duration 9600 Series IP Deskphones will display the appropriate message on the phone screen.

History

The History screen displays the calls that the user makes from and receives on the deskphone.

The user can select to see one of the following types of call history:

- All Calls

- Answered Calls
- Missed Calls
- Outgoing Calls

The user can get information about the Caller ID, Caller number, time and date of the call, and call duration.

Call treatment in a logged out state and busy Call Appearances

If a deskphone gets a call when all Call Appearances are busy, the deskphone does not display the incoming call, but the deskphone records the call as a missed call and displays it on the History screen.

If a deskphone gets a call when the user is not logged in, the system saves the incoming call in a database. When the user logs in again, the deskphone displays the previous call log and the calls received in the logged out state.

You need to configure the Call Log feature through System Manager. The Call Log feature has the following limitations:

- The Call Log feature is available only when the deskphone is connected to the primary Session Manager.
- When a user logs into multiple devices through the Mulitple Device Access (MDA) configuration, the History screens might not be synchronized between devices. If the user deletes Call Logs from the History screen in one MDA device, the other MDA devices might not clear the Call Logs from the History Screen.
- If the user disables the Call Log feature locally on the deskphone, call logs are stored on the server. When the user enables the Call Log feature, all call logs might show up.
- The deskphone does not display the Group Page calls with the name of the initiator of the Group Page, but with the name Group Page.
- Calls that come to deskphones that are redirected might not show the complete set of History details.

Customizing ring tones

There are fourteen (14) standard ring tones, eight (8) classic, and six (6) rich ring tones available for setting. The ring tones are set on the Personal Profile Manager (PPM). Ring tones for external, internal, priority, and intercom calls (distinctive ringing) are combinations of specified frequency, duration and cadence values. You can replace the eight (8) classic ring tones with the Korean ring tones or the customized ring tones.

Korean ring tones

Korean ring tones are part of the SIP software bundle download. To administer all or any of these tones to replace the existing external, internal, priority and intercom call tones, set the

EXTEND_RINGTONE parameter in the settings file with the names of the Korean tones you want available to the user. For example, to replace all the Avaya classic ring tones with the Korean ring tones, set the EXTEND_RINGTONE parameter to Korean ring tone XML files as follows:

```
SET EXTEND_RINGTONE = KoreanRT1.xml,KoreanRT2.xml,KoreanRT3.xml,KoreanRT4.xml,
KoreanRT5.xml,KoreanRT6.xml,KoreanRT7.xml,KoreanRT8.xml
```

To administer only the second and fourth Korean ring tones to replace the second and fourth Avaya standard tones, you would specify (without spaces between entries) :

```
SET EXTEND_RINGTONE = KoreanRT2.xml,KoreanRT4.xml
```

Note:

Do not include space between the XML file names.

Customized ring tones

A Ringtone Creation Tool in file `ringtone.xls` is included with the software download package. Use this tool to create XML files for up to eight custom ring tones as described in this section. Then:

- Save the custom ring tones to an HTTP server,
- Set the EXTEND_RINGTONE parameter with the name(s) of the XML file(s) you created,
- Reboot the deskphone to make the custom tone(s) available to the end user through the Avaya (A) Menu -> Options & Settings -> Screen & Sound option.

Important:

When setting up multiple ring tone files using the EXTEND_RINGTONE parameter, be sure that there are no spaces before or after the comma separating the filenames.

To create a custom ring tone, open the Ringtone. XLS spreadsheet and provide a value for each of the cells/fields in Ring tone XLS cell descriptions. A sample spreadsheet follows the table for illustration purposes only.

Ring tone XLS cell descriptions

Cell Name	Description	Comment
Ringer Name	Name of this custom Ring Tone file, for example, Ringtone 1	This filename will be assigned a .XML extension upon completing all required cells and pressing the "Create xml" cell button.

Table continues…

Cell Name	Description	Comment
Ringer Index	This numbers the xml file as one of the 8 patterns used in personalized ringing. For example, index 2 will be the second personalized ringing choice a user will have on their deskphone. Eight xml files with indices 1-8 need to be created to customize all the available personalized ringing choices that will be presented on a deskphone. If less than 8 indices/files are set in the settings file, Avaya standard ringing patterns will be used for the missing indices.	
Type of Wave	Leave empty; this cell is not currently used.	Reserved for future use.
Number of Active Frequencies	Up to four active frequencies can be set. Valid values are 1, 2, 3, or 4.	
Frequency Values	The range of frequency values is from 0 to 3999Hz.	
Number of Notes	Number of notes in this ring tone, from 1 to 3. A note is an interval in which a frequency is used. Currently, a custom ring tone has a 3 note maximum.	
Note 1, 2, and 3	This value represents a collection of frequency intervals that are grouped together and repeated over and over again as the ring tone	
Note Pulse State	The pulse state has two possible settings - On or Off	
Note Frequency	The frequency used for a particular note.	
Note Duration	The duration of the note in milliseconds, from 0 to 2^16.	
Next Note	Leave empty; this cell is not currently used.	Reserved for future use.
Cadence Patterns and States	Cadence patterns are set for internal, external, priority, and intercom calls.	

Table continues…

Cell Name	Description	Comment
Cadence 1 to 8	The number of available cadences.	
Cadence Duration	The duration of the cadence in milliseconds, from 0 to 2^16.	
Next Cadence	The next cadence is executed after the current cadence value is completed. This is used to create a loop of notes. For example, if number 1 is used for cadence state 8, when cadence 8 is completed, cadence 1 will follow.	
Cadence Next Index	Leave empty; this cell is not currently used.	Reserved for future use.
Reserved for future use.	When all applicable cells have been filled in, use this control to create an xml file for this specific tone.	

Downloadable ringtones

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

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

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

Ensure that audio files must:

- Be single-channel WAV files.
- Have encoding as per ITU-T G.711 A-law or u-law PCM with 8-bit samples at 8 kHz or 16-bit samples at 16 kHz.
- Have a maximum size of 512 KB.

- Have a combined size of not more than 5 MB.
- Only contain ASCII characters in their file names.

For example,

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

Administering voice mail

Set the MSGNUM parameter for configuring the **Messages** button. Configure the MSGNUM parameter with one the following:

- A standard telephone number the phone should dial to access your voice mail system, such as AUDIX or Octel.
- A Feature Access Code (FAC) that is configured for the Feature "To Voice Mail" will allow the user to transfer the active call directly to voice mail. FACs are supported only for QSIG-integrated voice mail systems like AUDIX or Octel. QSIG is an enhanced signaling system that allows the voice mail system and Communication Manager Call Processing to exchange information.

When the user presses the **Messages** button on the phone, that number or FAC is automatically dialed, giving the user one-touch access to voice mail.

The settings file specifies the phone number to be dialed automatically when the user presses this button. The command is:

```
SET MSGNUM 1234
```

where `1234` is the Voice Mail extension (Communication Manager hunt group or VDN).

However, when the phone is in failover mode, the phone might need to dial a different number to reach the voice mail system. Administer the parameter PSTN_VM_NUM to access the voice mail system through the Message button, while the phone is in failover mode. For example, during failover, the phone dials the public access number `345-555-1234` to access the voice mail at 1234. In this case, the command would be:

```
SET PSTN_VM_NUM 913455551234
```

Note:

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

Administering Presence

Presence overview

Presence is a feature that indicates the availability status of a contact. The phone periodically publishes its own presence status and retrieves the presence status of a contact from Avaya Aura® Presence Services.

Presence services facilitates aggregation of presence information collected from the following resources:

- Application Enablement ServicesServices
- Microsoft Office™ Communicator Server
- eXtensible Messaging and Presence Protocol (XMPP) Server

Presence services categorizes users into two types:

- **Watcher**: A user who is viewing the presence status.
- **Presentity**: A contact whose presence status is being viewed. Presentity is also referred to as Buddy.

A user can simultaneously be a Watcher and Presentity.

Users can manually set their own presence through the phone menu. You can configure the phone to use the Send All Calls (SAC) feature when the user sets the Do Not Disturb (DND) status.

Access Control List

The Access Control List specifies whether other users on the network can view the presence of another user. By default, users can automatically see the presence of other users. You can disable the automatic viewing by setting the `PRESENCE_ACL_CONFIRM` parameter in the `46xxsettings` file.

The phones that are in 1XC Shared Control Mode with a 1XC soft client can control automatic viewing. The 1XC softclient displays a popup window to the presentity that prompts whether to allow or to restrict the display of the presence information.

Presence profile

Presence profile is a part of the communication profile of a user. Presence profile is configured in **User Profile Management** of Avaya Aura® System Manager. In cluster deployment of multiple presence servers, presence profile explicitly associates a user with a presence server instance. The `46xxsettings.txt` file supports the use of only one presence server address. Using presence profile is an efficient method to ensure that a user is connected to the appropriate presence server. For information about configuring a presence profile, see *Avaya Aura® Presence Services*.

Avaya Aura® Call Center Elite features

The 9600 SIP software supports Avaya Aura® Call Center Elite features on 9600 Series IP Deskphones models 9608, 9608G, 9611G, 9621G, 9641G, and 9641GS. Avaya Aura® Call Center Elite 6.2 is the minimum requirement to support the following Call Center Elite features:

- Agent login/logout
- Agent greetings
- After call work
- Auxiliary work
- Auto and Manual in
- CC-Info agent event package
- Third party MWI
- Stroke counts
- Call work codes
- Display active VDN name
- VuStats
- Accept and display ASAI UUI information
- Forced logout override
- Supervisor assist
- Service observe
- QStats
- Interruptible AUX work

For detailed information on all the Call Center features, see *Using Avaya 96X1 SIP Agent Deskphones with Avaya Aura® Call Center Elite*, and *Administering Avaya Aura® Call Center Elite*, available on the Avaya support Website www.avaya.com/support.

You can assign the **Call Center** button features through PPM. The system displays these buttons in the Feature screen, button module, Quick Touch Panel, Phone screen, and the Home screen.

You can administer the Call Center features through the settings file using the following parameters:

Parameter name	Parameter Description
SKILLSCREENTIME	Sets the duration for which the deskphone displays the Skills screen
ENTRYNAME	Sets the entry name as the calling party name or the VDN or Skills name.

Table continues…

Parameter name	Parameter Description
UUIDISPLAYTIME	Specifies the duration for which the deskphone displays the user to user information (UUI) screen.
CC_INFO_TIMER	Sets the CC-Info event package timer.
BUTTON_MAPPINGS	Specifies a list of Button=Status pairs that change the operation of some of the buttons on the phone. Valid Button values are "Forward", "Speaker", "Hookswitch", and "Headset". Valid Status values are "na" and "cc-release". The default is null.

Agent Greeting

With this feature, you can configure any phone in your system to support Agent greetings in call center environment. When this feature is enabled, users logged in as Agents can record greeting messages with their own voice and play them back manually or automatically for incoming calls. Users can configure up to 6 greetings, each up to 10 seconds long and save them locally on the phone.

As an admin, you can configure whether the phone deletes or keeps recorded Agent greeting settings after the Agent logs out. You can also configure a backup location for the recorded messages. Use the following parameter to configure message storage server:

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

Agents can access and automatically download their messages when logging into another phone (hoteling).

You can configure this feature only in the `46xxsettings.txt` file.

This feature is available on Avaya J169/J179 IP Phone and Avaya J189 IP Phones.

Related links

Agent Greetings parameters on page 112

Agent Greetings parameters

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

Parameter name	Default Value	Description
AGTGREETINGSTAT	0	Specifies whether the Agent Greetings feature is enabled or not. Value operation: • 0: Disabled • 1: enabled

Table continues…

Parameter name	Default Value	Description
AGTGREETLOGOUTDEL	5	Specifies whether the phone deletes agent greeting messages upon the agent logout. • 0: The phone deletes agent greeting messages. • 1: The phone saves agent greeting messages.
AGENTGREETINGSDELAY	0	Specifies delat time in milliseconds between call pickup and agent greeting message playback start. Valid values are 0-3000

Related links

Agent Greeting on page 112

Team Button overview

The Team Button feature provides the facility to watch or monitor the phone of another user. The feature is configured on Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

By pressing the **Team** softkey, a user can do the following:

- Make a speed dial call to the monitored phone when it is free.
- Transfer an active call to the monitored phone.
- Monitor whether the phone redirects calls to any other phone.
- Monitor whether the phone has an active call.
- Answer a call that rings on the monitored phone.

The Team Button feature is configured on the Avaya Aura® Communication Manager and Avaya Aura® Session Manager. You can customize the ring type for Team Buttons on a monitored phone through a system parameter: TEAM_BUTTON_RING_TYPE.

Team Button parameters

Parameter	Default value	Description
TEAM_BUTTON_REDIRECT_INDICATION	0	Controls if the redirection indication is shown on a Team Button on a monitoring station. Valid values are 0 and 1.
TEAM_BUTTON_REDIRECT_OVERRIDE	0	Specifies whether the monitoring deskphone can override the SAC, CFWD, ECF features set by the monitored deskphone. Valid values are: • 0: Monitoring deskphone cannot override the features. • 1: Monitoring deskphone cannot override the features by placing the call to the monitored deskphone. • 2: Monitoring deskphone displays a message to the user asking if the call should be placed to the monitored deskphone. **Note:** The value of this parameter is stored in PPM.
TEAM_BUTTON_RING_TYPE	3	Specifies the default ring tone for all **Team Buttons**. Valid values are 1 to 8.
TEAM_BUTTON_RING_TYPE_PER_BUTTON	NULL	Specifies a list of name-value pairs that indicate default ring tones.

Team Button override

The monitored phone might have the call redirection feature active through one of the following features:

- Send All Calls
- Call Forward
- Enhanced Call Forward

You can configure Avaya Aura® Communication Manager and Avaya Aura® Session Manager so that the monitoring phone overrides the call redirection active on the monitored phone. If the call redirection override is set, the monitored phone rings for 30 seconds. If no one answers the call, the call is automatically sent to the redirection number.

Direct Transfer

The Direct Transfer feature provides the facility to transfer an active call to the monitored station.

When a call is answered at a monitoring phone, the user can begin the process of transferring the call to the monitored station by pressing the line corresponding to the Team button. The monitoring phone puts the existing call on hold and places a call to the monitored station. A speech path is established, and the monitoring station and monitored station can interact.

To complete the transfer between the original call and the monitored phone, the user at the monitoring station can disconnect the call by going on-hook or pressing the **Complete** softkey.

Direct Transfer is applicable only to the Team Button feature, and you need not configure the Direct Transfer feature on Avaya Aura® System Manager.

Enhanced Call Forward

The Enhanced Call Forward (ECF) feature provides flexibility to forward incoming calls to different destinations, based on the following different conditions:

- Caller type: Whether the call is coming from internal number or an external number.
- Phone status: Based on the phone status a user can choose to forward the calls in the following scenarios:
  - All incoming calls.
  - When the phone is busy.
  - When there is no answer on the phone.

You can set the **ECF** feature button for the phone to display on the Feature Screen, Quick Touch Panel, SBM24, BM12, Favorite Feature on the Phone Screen, or the Home Screen. Use the **ECF** feature button to access and enable or disable ECF.

Advanced call conference

In collaboration with the Avaya Aura® Conferencing server and Communication Manager, SIP release 6.5 or later provides advanced call conference features to the end user.Avaya Aura® Conferencing 7.0 is the minimum requirement to support advanced call conference. See the following table for a comparison of the advanced call conference features with different conference servers:

Feature	AST	AAC7
Participant list	No	Yes

Table continues…

Feature	AST	AAC7
Participant drop	Last party drop	Selective drop
Add participant	Single dial	Dial group
Voicemail	No filter	Voicemail
Number of participants	6	Unlimited
What is displayed	Number of participants, on the call appearance line, or on the Top Line.	The Details screen displays up to 25 participant names and their presence status. The Phone screen or the Top Line displays the total number of participants.
Selective mute	No	Yes

To enable advanced call conference features, you must first set the following parameters through the settings file:

- CONFERENCE_FACTORY_URI
- CONFERENCE_SERVER_ADDRESS
- CONFERENCE_SERVER_PORT
- ENABLE_SECURE_HTTP_FOR_CONFERENCING_SERVICE

Note:

SIP 6.5 does not support non-AST servers as primary controller for conferencing.

Assured services SIP

The Assured services SIP (AS-SIP) contains the following features:

Multi-Level Precedence and Preemption

The Multi-Level Precedence and Preemption (MLPP) feature is provided for the “dsn” and “uc” network of the U.S. DoD and Canadian DND. With this feature, users can place calls at various levels of precedence. Users are notified with precedence tone upon receiving incoming precedence calls. Higher precedence calls preempt the lower precedence calls when a user has no idle call appearance. Five precedence levels are supported for the “dsn” and “uc” network domains: Routine, Priority, Immediate, Flash, and Flash Override.

DSCP

The DSCP feature classifies outgoing traffic from SIP phones by marking each outgoing packet with a DSCP value. User signaling packets are marked according to the value of the DSCPSIG configuration parameter. Audio packets are marked with a DSCP value that is converted from the Precedence or Priority level of each call when the MLPP feature is enabled. OA&M packets are marked with the value of the DSCPMGMT configuration parameter.

Blind Transfer

With the Blind transfer feature, users can transfer an active call to another party without consultation.

Setting a large font size for the display

About this task

Use the following procedure to display the English language text in a larger font on the phone display. When you configure the large fonts feature, the phone displays the **Text Size** option in the **Options & Settings** menu. The large text size setting applies to the phone display as well as any attached button modules.

Before you begin

Ensure that the file `Mlf_Englarge.xml` resides on the web root of the HTTP Server.

Procedure

Modify the settings file to set the LANGLARGEFONT parameter as follows:

```
SET LANGLARGEFONT "Mlf_Englarge.xml"
```

Setting the background logo

About this task

Use the following procedure to set a customized background logo. The phone models 9608, and 9608G do not support a background logo.

Before you begin

Ensure that you have set the parameter LOGOS in the settings file.

Procedure

Modify the settings file to set the CURRENT_LOGO parameter to one of the labels specified in the LOGOS parameter.

When the logo file is not configured correctly or the HTTP server containing the logo file is not reachable, the phone might be temporarily unavailable.

In Avaya Aura® System Manager 6.3.8 or later, you cannot use this parameter if you are using the Expanded Template support for SIP Endpoints feature.

Background logo specifications

The following table specifies the information on the maximum size, color depth and format of a logo supported by the phone models 9611G, 9621G and 9641G. The phone models 9608, and 9608G do not support a background logo.

Models	Maximum size (pixels)	Color depth (bit)	Format
9611G	217 x 130	16	JPG
9621G, no QTP configured	232 x 140	16	JPG
9621G, 1 QTP configured	232 x 106	16	JPG
9621G, 2 QTP configured	232 x 72	16	JPG
9641G, no QTP configured	232 x 140	16	JPG
9641G, 1 QTP configured	232 x 106	16	JPG
9641G, 2 QTP configured	232 x 72	16	JPG

The following table specifies the information on the maximum size, color depth and format of a logo supported by the phone models 9611G, 9621G and 9641G for Call Center agents. The phone models 9608, and 9608G do not support a background logo.

Models	Maximum size (pixels)	Color depth (bit)	Format
9611G	217 x 96	16	JPG
9621G, no QTP configured	232 x 100	16	JPG
9621G, 1 QTP configured	232 x 66	16	JPG
9621G, 2 QTP configured	232 x 32	16	JPG
9641G, no QTP configured	232 x 106	16	JPG
9641G, 1 QTP configured	232 x 72	16	JPG
9641G, 2 QTP configured	232 x 38	16	JPG

Service Observe

In the call center environment, a supervisor can use the Service Observe feature to perform the following:

- Monitor a phone call to observe the call quality.
- Talk to the agent and the customer.
- Silently coach the agent during the service observation.

You can configure the feature using Avaya Aura® System Manager. For more information, see Avaya Aura® System Manager documentation.

Use the Computer Telephony Integration(CTI) client to remotely activate or deactivate the feature. For more information, see Avaya Aura® Application Enablement Services documentation.

WML browser overview

WML browser feature comparison

The phones have an built-in WML browser application. Users can see the browser application listed in the **Home** screen of Avaya menu, if the related system parameters are configured in the `46xxsettings.txt` file.

The following table shows a comparison of different features of the WML browser across the phone models.

Feature	9608/9608G	9611G	9621G	9641G/9641GS
Top line	Yes	Yes	Yes	Yes
Application lines	4	4	4	5
Line buttons	Yes	Yes	No	No
Selectable objects per line	1	1	1	1
Application line height (in pixels)	15	31	38	38
Softkeys per screen	4	4	5	5
Softkey height (in pixels)	14	31	38	38
Navigation buttons	Yes	Yes	No	No
Text input	Yes	Yes	Yes	Yes
Color support	No	Yes	Yes	Yes
Supported image format	JPEG	JPEG	JPEG	JPEG

Table continues…

Feature	9608/9608G	9611G	9621G	9641G/9641GS
Max image width (in pixels)	175	300	430	430
Click to dial	Yes	Yes	Yes	Yes
Add to phonebook	Yes	Yes	Yes	Yes
Characters per line (normal font)	31	40	39	39
Characters per line (large font)	25	22	26	26
Characters per softkey (normal font)	8	8	8	8
Characters per softkey (large font)	6	6	8	8

Microsoft Exchange Server integration

Phones can connect with Microsoft Exchange Server. With this connection, users can do the following:

- View calendar reminders to make a call that users can dismiss or snooze. Users can also use the reminders to make a call.
- Dial into conference calls without entering a conference call number and access code.
- View exchange contacts.

Note:

Exchange Web Services is supported for Microsoft Exchange Server 2010 or later.

You can secure the link between the phones and the Exchange server. The phone adds the Exchange contacts of a user to the contact list and displays it in the Exchange Contacts screen. Users can save the Exchange contacts to PPM using the +Local key. To gain access to the Exchange contacts, calendar, and reminder information, users must use Avaya Menu to specify the following information:

- Credentials
- Display preferences
- Calender date

Users can modify or delete contacts that are saved in PPM. Avaya SIP phones do not support the presence tracking feature for the Exchange contacts.

Microsoft Exchange parameters

Parameter name	Default value	Description
PROVIDE_EXCHANGE_CALENDAR	1	Specifies whether menu items for Exchange Calendar are displayed. Value operation: • 0: Not displayed • 1: Displayed
PROVIDE_EXCHANGE_CONTACTS	1	Specifies whether menu items for Exchange Contacts are displayed. Value operation: • 0: Not displayed • 1: Displayed
EXCHANGE_AUTH_METHOD_DEFAULT	0	Specifies the Exchange authentication method configured by administrator. When you configure Basic (Forced) or OAuth (Forced) method, it is the active authentication method. The phone user is not allowed to change the authentication method from phone user interface. When you configure non-forced method, phone user can change the authentication method from the phone user interface and configure the active authentication method. Value operation: • **0**: Basic authentication (Default) • **1**: OAuth authentication • **2**: Basic authentication- forced • **3**: OAuth authentication- forced
EXCHANGE_SERVER_LIST	outlook.office365.com	Specifies a list of one or more Exchange server IP addresses. Addresses can be in dotted-decimal or DNS name format, separated by commas without any intervening spaces. The list can contain up to 255 characters.

Table continues…

Parameter name	Default value	Description
EXCHANGE_USER_ACCOUNT_DEFAULT	Null	Specifies the Exchange user account configured by administrator. This parameter is only applicable when authentication method is OAuth. If phone user hasn't configured any user name on the phone user interface then value configured in this parameter would be used. The valid value is a string of up to 255 characters. The default value is empty.
EXCHANGE_USER_DOMAIN	Null	Specifies the domain for the URL used to obtain Exchange contacts and calendar data. The parameter is used as a part of the user authentication. The value can contain 0 to 255 characters. You can change the value by using the Admin menu on the phone.
ENABLE_EXCHANGE_REMINDER	0	Specifies whether or not exchange reminders will be displayed. Value Operation: • 0: Not displayed • 1: Displayed
EXCHANGE_REMINDER_TIME	5	Specifies the number of minutes before an appointment at which a reminder will be displayed. Valid values are 0 through 60.
EXCHANGE_SNOOZE_TIME	5	Specifies the number of minutes in which a reminder must be displayed again after it is temporarily dismissed. Valid values are 0 through 60.
EXCHANGE_NOTIFY_SUBSCRIPTION_PERIOD	180	Specifies the number of seconds between re-syncs with the Exchange server. Valid values are 60 through 3600.
EXCHANGE_EMAIL_DOMAIN	Null	Specifies the Exchange email domain. The value can contain 0 to 255 characters.
EXCHANGE_SERVER_SECURE_MODE	1	Specifies if HTTPS should be used to contact Exchange servers. Value Operation • 0: Use HTTP • 1: Use HTTPS

Table continues…

Parameter name	Default value	Description
EXCHANGE_SERVER_MODE	3	Specifies the protocol to be used to contact Exchange servers. Value Operation: • 1: Use WebDAV • 2: Use Exchange Web Services (EWS) • 3: Try EWS first, if that fails, try WebDAV (default)

Resetting system values

About this task

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

⚠ Caution:

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

Procedure

1. Select RESET VALUES from the screen. The phone displays the following text:
2. Press one of the following:
   - **Reset**: To start the phone reset.
   - **Cancel**: To return to the previous screen.

   The phone resets from the beginning of registration, which might take a few minutes. The phone resets:
   - All system values and system initialization values except AUTH and AUTH_ONLY to default values.
   - The 802.1X ID and Password to their default values.
   - Call server values to their defaults.
   - Any entries in the Redial buffer.
   - Does not affect user-specified data and settings like Contacts data or the phone login and password.

Clearing the phone settings

About this task

Sometimes, you might want to remove *all* administered values, user-specified data, and option settings and return a phone to its factory settings. You might have to remove all administered values when you give a phone to a new, dedicated user and when the **LOGOFF** option is not sufficient. For example, a new user is assigned the same extension, but requires different permissions than the previous user.

The **CLEAR** option erases all administered data—static programming, HTTP and HTTPS server programming, and user settings including Contact button labels and locally programmed Feature button labels, and restores all such data to default values. Using the **CLEAR** option does not affect:

- The software load. If you upgrade the phone, the phone retains the latest software. After you clear a phone of the settings, you can administer the phone normally.

Caution:

This procedure erases all administered data without any possibility of recovering the data. Neither the boot code nor the application code is affected by this procedure.

Use the following procedure to clear the phone of the administrative, user-assigned, and options values.

Procedure

1. Select **CLEAR** from the menu.

   The phone prompts for confirmation.

2. Press one of the following:

   - **Clear**: To clear all values to use initial default values.
   - **Cancel**: If you do not want to clear all values and to terminate the procedure and retain the current values.

   The phone displays the following text:

   ```
   Clearing values...
   ```

   The phone is reset to the default factory settings.

   - All system values and system initialization values.
   - 802.1X identity and password.
   - User options, parameter settings, identifiers, and password.

   After clearing the values, the phone resets.

Restarting the phone

About this task

Use the following procedure to restart the phone.

Procedure

1. Use the CRAFT password to gain access to the Administration procedures screen. The default password is *27238*.
2. When you select **RESTART PHONE** from the Administration procedures screen, the phone displays a confirmation screen with the following message:

   ```
   Are you sure you want to restart the phone?
   ```

3. Press **No** to return to the Administration procedures screen without restarting the phone. Press **Yes** to proceed with the registration steps

   A restart does not affect user-specified data and settings like Contacts data or the phone login and password.

   The remainder of the restart procedure depends on the status of the boot and application files.

Contacts list

With the Contacts application, users can manage their phone contacts list. Users can view and edit their contacts and select a contact name or number to make calls. Users can also create and update contact groups with the entries available in the Contacts list and search for users in an LDAP directory.

Following are the types of contacts:

- Local contacts: Contact stored locally on the phone.
- System contacts: Contacts in a company directory or database.
- Global Exchange contacts: Contacts in a company exchange directory.
- Personal Exchange contacts: Contacts in a user personal exchange account.
- Microsoft® Exchange contacts: Contacts in a Microsoft® Exchange account.

To enable the contact feature and access to modify the contacts, see, Applications and features provisioning.

Related links

Applications and features provisioning on page 61

LDAP Directory

The LDAP Directory feature allows users to search contacts in any LDAP directory. When this feature is enabled, LDAP search appears in Contacts application on the phone. You can set up the parameters for an LDAP directory server using the web interface and the `46xxsettings.txt` file.

When searching for a contact, users can specify attributes in a search query and view up to 49 attributes for each match. The set of attributes depends on the selected LDAP server.

Users can select an LDAP server as a contact search source in **Applications** > **Contacts** > **Search** > **Sources**. When enabled, LDAP becomes the only available contact database, other contact databases are disabled.

Users can search any public LDAP directory that does or does not require authentication.

The user can successfully connect to the selected LDAP server using ldaps:// protocol if the following settings are configured:

- DIRSECURE=2
- DIRSRVRPRT corresponds to LDAPS port of the server
- DIRSRVR is FQDN
- Root CA certificate that issued the LDAP server certificate is included in the TRUSTCERTS list

Chapter 6: 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 the 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 multiple proxies This makes the method of redundancy quick and deterministic. While configuring the phones for redundancy with Avaya Aura®, set the parameter SIPREGPROXYPOLICY to Simultaneous. 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. However, 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, the value of SIMULTANEOUS_REGISTRATIONS is 2.

Limitations during failover or failback

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

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

Preserved call

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

Limitations of call preservation

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

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

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

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

Supported non Avaya Aura® proxies for redundancy

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

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

Note:

All secondary gateways must be configured to support connection reuse.

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

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

Note:

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

Preserved call

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

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

Table continues…

Parameter name	Default value	Description	System Manager parameter name
DISCOVER_AVAYA_ENVIRONMENT	1	Specifies dynamic feature set discovery Value operation: • 1: The phone discovers and verifies if the controller supports the AST feature set or not. The phone sends a SUBSCRIBE request to the active controller for the Feature Status Event Package (avaya-cm-feature-status). If the request succeeds, the phone proceeds with PPM Synchronization. If the request is rejected, or is proxied back to the phone, or does not receive a response, the phone assumes that AST features are not available. • 0: The phone operates in a mode where AST features are not available. **Note:** Set the parameter to 0 for IP Office environment.	NA
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

Table continues…

Parameter name	Default value	Description	System Manager parameter name
ENABLE_PPM_SOURCED_SIPPROXYSRVR	1	Enables PPM as a source of SIP proxy server information. Value operation: • 0: Proxy server information received from PPM is not used. • 1: Proxy server information received from PPM is used.	NA
SIP_CONTROLLER_LIST_2	Null	Replaces SIP_CONTROLLER_LIST for IPv4 and IPv6 phones. It is used to select the registration address.	Primary Session Manager, Secondary Session Manager, and Survivability server.
SIMULTANEOUS_REGISTRATIONS	3	Specifies the number of simultaneous Session Manager and Branch Session Manager registrations that the phone must maintain. The 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	Simultaneous	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. This value is supported only in IP Office environment. • Simultaneous: The phone simultaneously registers to more than one SIP proxy controller at the same time. This value is supported only in Avaya Aura® environment	NA

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

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

Parameter name	Default value	Description
ENABLE_REMOVE_PSTN_ACCESS_PREFIX	0	Enables the removal of the PSTN access prefix from the collected dial strings when the phone communicates with a non-AST controller. 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.

Table continues…

Parameter name	Default value	Description
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 numbers with more flexibility when used together with the LOCAL_DIAL_AREA_CODE parameter .
PHNDAC	Null	Dial access code - will be applied if the dialed number length + the length of the Dial access code length equals the national number length. This calculation does not include an outside line access code. It is different from PHNLAC since PHNLAC is applied when the phone number length is more than ext number length and less than national number length.
LOCAL_DIAL_AREA_CODE		Specifies whether a user must dial the area code for calls within the same area code regions. 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 only supported in Broadsoft environment.

Chapter 7: Backup and restore

User profile backup on Personal Profile Manager (PPM)

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

To support the data backup, the phone saves all the user settings on the PPM in an Avaya Aura® environment. When the user logs in to any registered device, PPM restores all user data on the device.

User profile parameters for backup

The table lists the parameters that are backed up on PPM. These are internal parameters corresponding to the user settings on the phone and not available on the `46xxsettings.txt` file.

Parameter	Default value	Description
BAKLIGHTOFF	120	Specifies the timer to switch off the backlight of the display.
CLICKS	1	Specifies if the phone button can generate click sounds.
CALL_PICKUP_RING_TYPE	1	Specifies the default call pickup ring type.
OUTSIDE_CALL_RING_TYPE	1	Specifies the default outside call ring type.
FORWARDED_CALL_RING_TYPE	1	Specifies the default forwarded ring type that the user selects.
CALL_PICKUP_INDICATION	3	Specifies the following call pickup indication types: • Audio • Visual • None
TIMEFORMAT	0	Specifies whether the time format is the am-pm format or the 24–hour format.

Table continues…

Parameter	Default value	Description
DATE_FORMAT_OPTIONS	1	Specifies the date display format.
CALL_LOG_ACTIVE	1	Specifies whether to activate call logging.
CONTACT_NAME_DISPLAY	1	Specifies how contact names are displayed.
DEFAULT_CONTACTS_STORE	1	Specifies the account where all user contacts are added by default.
ENABLE_PHONE_LOCK	0	Specifies whether a softkey and a 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.
AUDIOPATH	1	Specifies whether the default audio path is speaker or headset.

Chapter 8: Phone upgrade

Device upgrade process

The upgrade event is logged under NOTICES level in the Syslog file. During boot up, the 9600 Series IP Deskphones performs the following tasks:

1. The phone receives the file server address from DHCP, LLDP, or the device interface.
2. The phone connects to the file server and searches for the upgrade file depending on the SIG parameter value.
   - 0: Default, `96x1Supgrade.txt`
   - 1: H.323, `96x1Hupgrade.txt`
   - 2: SIP, `96x1Supgrade.txt`
3. The phone compares its software version with the version specified in the upgrade file.
   - For Sonic and other hardware phones, HWVER value is also checked when the MODEL4 match is found.
4. The phone then downloads the upgrade file for parsing. The parameter UPGRADE_FILE_EXECUTION_STATUS is updated with the following values upon parsing:
   - 0: Upgrade file is downloaded and parsed.
   - 1: Upgrade file is downloaded but not parsed.
   - 2: Upgrade file is not downloaded and not parsed.
5. The upgrade gets triggered depending on the parameter UPGRADE_FILE_EXECUTION_STATUS value.
6. The phone starts downloading files depending on the parameter APPNAME value contained in the upgrade file.

   Tip:

   The software files contain three binaries BootA, BootB, and System RFS. Each binary contains a version number and a signature header which is processed in sequence and is stored in the appropriate flash memory location.
7. The phone downloads the software files and upgrades itself if no fatal error occurs.

Tip:

Fatal error occurs when the file size is too large, missing signature or if the signature validation fails, file is not found, file download failure, fails to write to the flash memory, file is incompatible with the hardware, or during any parsing error.

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 .
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.

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. The only system values that can be used in the conditional statement are: BOOTNAME, GROUP, MACADDR, MODEL, and SIG.
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. Modify the `46xxsettings.txt file` as required.
10. Restart the HTTP/HTTPS server.
11. 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.txt` file before downloading a language file with the same filename.

Note:

Language files for SIP deskphones have a `.xml` filename extension whereas language files for IP phone set to H.323 have a `.txt` filename extension.

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.txt` 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 9: Data Privacy Controls Addendum

Purpose

Data privacy controls addendum applies to Avaya 96x1 Series IP Phones.

Personal Data is stored internally in the phone's flash file system which is not directly externally accessible except through SSH to the limited privilege "craft" user via an Avaya EASG login. Filesystem content is not encrypted except for passwords. When Personal Data is being transmitted over a network, it is encrypted with the most up-to-date protocols.

Related links

Configuring Data Privacy on the Avaya J179 IP Phone

Data categories containing personal data (PD)

User data (in memory)

Calls: Remote party phone number

Conference calls: participant display name, roster list

End user preferences information

Device configuration information

Contacts retrieved from network

User data (on flash)

Device configuration information

End user preferences information

Call Logs (on flash)

Local call logs

User Passwords (on flash)

User's SIP password, WiFi password, EAP password, http password, local Admin password

User data in logs (on flash)

User handle, SIP user name, display name information from SIP messages.

Personal data human access controls

User data (in memory)

- No Access

User data (on flash)

- SSH – Limited to Avaya Services login to the “craft” account with EASG authentication. “craft” account has limited access to filesystem.
- Web Admin – Access is limited to a predefined “admin” account where the password is defined by the customer. Access is provided to most configuration settings and some user settings.

Call Logs (on flash)

- No Access

User Passwords (on flash)

- No Access

User data in logs (on flash)

- SSH – Limited to Avaya Services login to the “craft” account with EASG authentication. “craft” account has limited access to filesystem.
- Web Admin – Access is limited to a predefined “admin” account where the password is defined by the customer. Access provides the ability to download a Phone Report which contains log files.

Related links

Personal data programmatic or API access controls on page 146

Personal data programmatic or API access controls

User data (in memory)

• Internal programmatic access.

User data (on flash)

• None

Call Logs (on flash)

•None

User Passwords (on flash)

•None

User data in logs (on flash)

•None

Related links

Personal data human access controls on page 146

Personal data at rest encryption controls

User data (in memory)

- Not encrypted by phone application except for passwords stored in memory. Passwords are only decrypted temporarily during use.

User data (on flash)

- Not Encrypted

Call Logs (on flash)

- Not Encrypted

User Passwords (on flash)

- AES-256 encrypted
- There are no controls available for the type or strength of encryption

User data in logs (on flash)

- Not Encrypted

Personal data in transit encryption controls

User data (in memory)

- TLS 1.2 to send/receive data with servers

User data (on flash)

- TLS 1.2 (HTTPs) to send/receive data with servers
- SSH

Call Logs (on flash)

- TLS 1.2 (HTTPs) to receive data with servers
- Data is never transmitted out of the phone

User Passwords (on flash)

- TLS 1.2 to send/receive data with servers (only the encrypted form is transmitted)

User data in logs (on flash)

- TLS 1.2 (HTTPs) to send data with servers when it is being sent as a phone report
- SSH

Personal data retention period controls

User data (in memory)

- In-memory data is removed based on use cases. For example, during a call, a call object remains in memory. When the call ends, the object is removed from memory, but a new CallLog object is created.

User data (on flash)

- Permanent until rolled over, or until the device is reset to defaults

Call Logs (on flash)

- Permanent until rolled over, manually deleted by the user, or until the device is reset to defaults

User Passwords (on flash)

- Permanent until rolled over, or until the device is reset to defaults

User data in logs (on flash)

- Permanent until rolled over, or until the device is reset to defaults

Personal data export controls and procedures

User data (in memory)

- Not applicable

User data (on flash)

- Using the phone Administration menu, an Administrator can generate a Phone Report containing configuration data which is transmitted if an external backup server is configured via the BRURI setting
- While logged in to craft via SSH, configuration data can be transmitted.
- While logged into an Admin Web page, configuration data can be viewed and exported or a Phone Report can be generated and saved.

Call Logs (on flash)

- No export capability is provided

User Passwords (on flash)

- No export capability is provided

User data in logs (on flash)

- Using the phone Administration menu, an Administrator can generate a Phone Report containing logs which is transmitted if an external backup server is configured via the BRURI setting
- While logged in to “craft” via SSH, log files containing user data can be transmitted
- While logged into an Admin Web page, log files containing user data can be exported

Personal data view, modify, delete controls and procedures

User data (in memory)

- Not applicable

User data (on flash)

- The User can modify and delete settings from the local menu on the phone
- The Administrator can modify and delete selected data using the Administration menu on the phone
- The Administrator can modify and delete selected data using the Admin web page

Call Logs (on flash)

- The User can delete individual log entries or all log entries from the local menu on the phone
- The Administrator can delete all call logs using the Reset to Defaults function in the Administration menu on the phone
- The Administrator can delete all call logs using the Reset to Defaults function in the Admin web page

User Passwords (on flash)

- The User cannot directly modify passwords
- The Administrator can delete all passwords using the Reset to Defaults function in the Administration menu on the phone
- The Administrator can delete all passwords using the Reset to Defaults function in the Admin web page

User data in logs (on flash)

- The User has no ability to modify or delete log files
- The Administrator can delete all log files in the phone using the Reset to Defaults function in the Administration menu on the phone
- The Administrator can modify and delete selected data using the Admin web page or delete all data using the Reset to Default function

Personal data pseudonymization operations statement

User data (in memory)

- Not applicable

User data (on flash)

- Not applicable

Call Logs (on flash)

- Not applicable

User Passwords (on flash)

- Not applicable

User data in logs (on flash)

- Not applicable

Data privacy and secure data processing

Avaya J100 Series IP Phones provide measures to ensure data privacy and secure processing of personal data. You can configure the phones in a secure mode to encrypt personal data at rest and end-to-end encrypt personal data in transit.

Secure mode

In secure mode, phones provide secure processing of personal data. Internal configuration files are encrypted and any internally generated logs and reports do not persist for longer than 24 hours. You can manually generate a new phone report in secure mode, but the phone deletes it 8 hours after its creation.

Secure mode activation

By default, Secure mode is off on the phones. You can activate secure mode by using one of the following methods:

- In the `46xxsettings.txt` file, set the ENABLE_GDPR_MODE parameter to `1`.
- In web interface, navigate to **Settings** > **Privacy** > **GDPR mode** and set it to `Enable`

Secure mode deactivation

You can deactivate Secure mode by using one of the following methods:

- In the `46xxsettings.txt` file, set the ENABLE_GDPR_MODE parameter to `0`.
- In web interface, navigate to **Settings** > **Privacy** > **GDPR mode** and set it to `Disable`

Related links

Configuring Secure Mode on the Avaya J179 IP Phone

Configuring secure mode parameter

You can configure the following parameter to enable secure mode.

Name	Default value	Description
ENABLE_GDPR_MODE	0	Specifies if data security and privacy mode is applied on the phone. When this parameter is enabled, the phone doesn't store any personal data without encryption for a period of more than 24 hours. Value operation: • 0: Secure mode is disabled (default) • 1: Secure mode is enabled

Data privacy

In addition to activating the secure mode, you must use the following configuration to ensure user data is private:

- Contacts: disable by setting the following `46xxsettings.txt` parameter:

  ```
  SET ENABLE_CONTACTS 0
  ```

- Recents: disable by setting the following `46xxsettings.txt` parameter:

  ```
  SET ENABLE_CALL_LOG 0
  ```

  Note:

  The phone deletes existing Recents logs when you apply this setting.

- Force HTTPS for configuration and disable Web Server: set the following `46xxsettings.txt` parameters:

  ```
  SET ENABLE_WEBSERVER 0
  ```

  ```
  SET AUTH 1
  ```

- Logs: by default, logs are protected, because the SSH server is disabled by default. Logs are internal to the phone and, with GDPR mode activated, are cleared every 24 hours. To maintain these settings, do not set the SET SSH_ALLOWED parameter value to other than 0. To protect logs, use the following `46xxsettings.txt` parameters:

```
SET SYSLOG_LEVEL 1
SET SYSLOG_ENABLED 0
SET LOGSRVR ""
SET LOG_CATEGORY ""
```

You can also enable the Secure Syslog feature. If you choose this option, use the following configuration:

`SET SYSLOG_ENABLED 1`

`SET LOGSRVR "xx"` where xx is an FQDN address for a TLS server.

Enable the Phone Lock feature

To enable the Phone Lock feature, you need to provide SIP login and password information to the user.

You can configure the Phone Lock feature so that users can manually lock their phones using the **Lock** soft key on the Idle phone screen or the **Lock** feature key. You can also set the idle time interval after which the phone automatically locks.

To do this, set the following `46xxsettings.txt` parameters:

- `SET ENABLE_PHONE_LOCK 1`
- `SET PHONE_LOCK_IDLETIME`: use any value other than 0 for this parameter to set the idle time interval.

Additional settings

The following settings are turned off by default, but if you want to ensure that data privacy is maintained as required, make sure you observe the following settings:

- `SET SNMPADD ” “`
- `SET TPSLIST ” “`
- `SET SLMSTAT ” “`

Use HTTPS values for the following settings:

- `USER_STORE_URI`
- `XSI_URL`
- `CONFIG_SERVER_SECURE_MODE` — do not set to 0

Use TLS values for the following settings:

- `SIP_CONTROLLER_LIST`
- `SIP_CONTROLLER_LIST_2`
- `SET SIPSIGNAL  2` — TLS is used by default
- `SET ENABLE_OOD_MSG_TLS_ONLY 1` — TLS is used by default

Secure Syslog

The Secure Syslog feature enables you to select between a secure and non-secure modes for syslog messages transportation. When you select the secure syslog mode, the phone carries out all syslog events reporting over a secure TLS channel. When you select the non-secure mode, the phone uses a UDP channel.

When in the secure syslog mode, the phone maintains the connection to the TLS server indefinitely. If the connection is lost, it begins to reconnect immediately until the connection is established.

If the phone receives a log message during a connection timeout, it discards the messages. The number of log messages lost due to the absence of connection is recorded in a separate local log entry.

You need to configure the following settings for the secure syslog TLS connection:

- ENABLE_PUBLIC_CA_CERTS: specifies whether embedded certificated are trusted or verified against the list defined by TRUSTCERTS.
- TRUSTCERTS: specifies a list of well-known public certificates.
- TLSSRVRID: specifies if the phone performs identity matching for trusted certificates.
- TLS_VERSION: specifies the version of the TLS protocol the phone uses.
- KEYUSAGE_REQUIRED: specifies if key usage extension is checked for.
- LOGSRVR: the value for this parameter must be an FQDN address when you select the secure syslog mode.

You can configure this feature using the `46xxsettings.txt` file, the web user interface and the phone Administrator menu.

Related links

Secure Syslog parameters on page 153

Secure Syslog parameters

Use the following `46xxsettings.txt` file parameters to configure the Secure Syslog feature.

Name	Default value	Description
LOGSRVR_SECURE	0	Specifies if the phone uses secure or non-secure syslog transport mode by default. Value operation: • 0: Non-secure mode using UDP transport • 1: Secure mode using TLS transport RFC 5425 Selected value is available as Default option in Administrator menu

Related links

Secure Syslog on page 153

Geographical restrictions on encryption

Starting from R.4.0.4., SRTP is not supported on Avaya J100 Series IP Phones sold in Russia, Belarus, Kazakhstan, Kyrgyzstan, and Armenia to meet local restrictions on the use of encryption.

On such phones, the settings related to SRTP are excluded both from the phone interface and the web interface, and the administrator cannot enable SRTP.

Chapter 10: Troubleshooting

SLA Mon™ agent

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

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

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

Note:

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

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

Error 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 156

Power interruption on page 156

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 155

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 155

Installation error and status messages

The 9600 Series IP Deskphonesissue 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. 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 phone continually reboots, or reboots continuously about every 15 minutes.	Cause: The phone cannot find the call server. Resolution: Ensure that SIP_CONTROLLER_LIST is administered either manually or through DHCP or HTTP, as appropriate.	
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, 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.

Table continues…

	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 Communication Manager call server, add or change NAT, etc.	Cause: Loss of communication with Session Manager. Resolution: As above.
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.

Table continues…

	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.
	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.	

Table continues…

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 ***96x1Supgrade.txt***file was edited incorrectly, renamed, etc. Resolution: Download a clean copy of the ***96x1Supgrade.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.	

Table continues…

	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 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".	

Table continues…

Login fails after phone upgrade, when Avaya Session Manager uses Identity certificate signed by Avaya SIP Root CA, TLSSRVRID is 1 in the `46xxsettings.txt` file or in the DHCP SSON Option 43	Cause: TLSSRVRID is enforced on any connection on R7.1.0 and on connections where SIP Root CA certificate is being used. Identity certificates signed by Avaya SIP root CA certificate are not unique and therefore if TLSSRVRID is set to 1 the SIP registration/PPM fails. Resolution: • Set TLSSRVRID to 0 if Avaya SIP Root CA is used. • Replace the identity certificate of the session manager or PPM to a new one where the SIP domain, defined by SIPDOMAIN, is found in the Subject Alternative Name and the SIP controller IP address or host name is found in the common name or Subject Alternative Name.
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.

Error handling and troubleshooting for certificate renewal

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

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

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

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

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

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

Related links

Identity certificate renewal on page 49

Chapter 11: Resources

Documentation

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

Title	Use this document to:	Audience
Overview		
9600 Series IP Deskphones Overview and Specifications	See characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security, and licensing requirements of the 9600 Series IP Deskphones.	People who want to gain a high-level understanding of the 9600 Series IP Deskphones features, functions, capacities, and limitations.
Avaya Aura® Session Manager Overview and Specification	See characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security, and licensing requirements of the Avaya Aura® Session Manager.	People who want to gain a high-level understanding of the Avaya Aura® Session Manager features, functions, capacities, and limitations.
Avaya Aura® Communication Manager Feature Description and Implementation	See characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security, and licensing requirements of the Avaya Aura® Communication Manager.	People who want to gain a high-level understanding of the Avaya Aura® Communication Manager features, functions, capacities, and limitations.
Avaya IP Office™ Platform Feature Description	See information about the feature descriptions.	People who perform system administration tasks.

Table continues…

Title	Use this document to:	Audience
Avaya IP Office™ Platform Solution Description	See information about how the products and services interoperate with this solution.	People who want to gain a high-level understanding of the IP Office features, functions, capacities, and limitations.
Implementing		
Deploying Avaya Aura® Session Manager	See the installation procedures and initial administration information for Avaya Aura® Session Manager.	People who install, configure, and verify Avaya Aura® Session Manager on Avaya Aura® System Platform.
Upgrading Avaya Aura® Session Manager	See upgrading checklists and procedures.	People who perform upgrades of Avaya Aura® Session Manager.
Deploying Avaya Aura® System Manager on System Platform	See the installation procedures and initial administration information for Avaya Aura® System Manager.	People who install, configure, and verify Avaya Aura® System Manager on Avaya Aura® System Platform at a customer site.
IP Office SIP Telephone Installation Notes	See the installation procedures and initial administration information for IP Office SIP telephone devices.	People who install, configure and verify SIP telephone devices on IP Office.
Administering		
Administering Avaya 9601/9608/9608G/9611G/ 9621G/9641G/9641GS IP Deskphones SIP	See information about performing 9600 Series IP Deskphones administration tasks, including how to use management tools, how to manage data and security, and how to perform periodic maintenance tasks.	People who perform 9600 Series IP Deskphones system administration tasks such as backing up and restoring data and managing users.
Administering Avaya Aura® Session Manager	See information about performing Avaya Aura® Session Manager administration tasks, including how to use management tools, how to manage data and security, and how to perform periodic maintenance tasks.	People who perform Avaya Aura® Session Manager system administration tasks.

Table continues…

Title	Use this document to:	Audience
Administering Avaya Aura® System Manager	See information about performing Avaya Aura® System Manager administration tasks, including how to use management tools, how to manage data and security, and how to perform periodic maintenance tasks.	People who perform Avaya Aura® System Manager administration tasks.
Administering Avaya IP Office™ Platform with Manager	See information about short code configurations for the feature list	People who need to access IP Office features using short codes.
Administering Avaya IP Office™ Platform with Web Manager	See information about IP Office Web Manager administration tasks, including how to use the management tool, how to manage data and security, and how to perform maintenance tasks.	People who perform IP Office Web Manager administration tasks.
Maintaining		
Maintaining Avaya Aura® Session Manager	See information about the maintenance tasks for Avaya Aura® Session Manager.	People who maintain Avaya Aura® Session Manager.
Troubleshooting Avaya Aura® Session Manager	See information for troubleshooting Avaya Aura® Session Manager, resolving alarms, replacing hardware, alarm codes, and event ID descriptions.	People who troubleshoot Avaya Aura® Session Manager.
Using IP Office System Status	See information about the maintenance tasks for System Status Application.	People who maintain System Status Application.
Using IP Office System Monitor	See information about the maintenance tasks for SysMonitor.	People who maintain SysMonitor.

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

7. Click **Enter**.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

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

Appendix A: List of configuration parameters

Parameter name	Default value	Description
100REL_SUPPORT	1	Specifies whether the 100rel option tag is included in the SIP INVITE header field. Value operation: • 0: The tag is not included. • 1: The tag is included.
A		
ACOUSTIC_EXPOSURE_PROTECT_MODE_DEFAULT	Off	Specifies the long-term acoustic exposure protection mode default setting. Value operation: • Off • Dynamic • 4 hours • 8 hours
ADMIN_HSEQUAL	1	Specifies handset audio equalization standards compliance. This parameter impacts the phone only if the handset equalization is not set by the user or by the HSEQUAL local procedure for that phone. Value operation: • 1: Use handset equalization that is compliant with TIA 810/920. • 2: Use handset equalization that is compliant with FCC Part 68 HAC requirements.

Table continues…

Parameter name	Default value	Description
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.

Table continues…

Parameter name	Default value	Description
ADMIN_PASSWORD	27238	Specifies an access code for accessing the Admin menu. Valid values are from 6 to 31 alphanumeric characters including upper case, lower case characters and special characters. However, double quote character (“) cannot be used for a value of this parameter. **Note:** • If this parameter length is set below 6 or above 31 alphanumeric characters, then the parameter is treated as not defined. • If this parameter is set in the `46xxsettings.txt` file, then it replaces PROCPSWD parameter. • If you set ADMIN_PASSWORD in the Avaya Aura® System Manager you require at least Avaya Aura® System Manager 7.1.0. • Setting this parameter through PPM is more secure because this file can usually be accessed and read by anyone on the network. Setting the value in this file is intended primarily for configurations with versions of phone or if server software that do not support setting this value from the server.
AMADMIN		Specifies the URI used for WML-applications under (AVAYA) Menu. You must specify HTTP server and directory path to administration file (`AvayaMenuAdmin.txt`). Do not specify the administration file name.

Table continues…

Parameter name	Default value	Description
ALLOW_DND_SAC_LINK_CHANGE	0	Specifies whether to enable DND and SAC link button in the menu. Value operation: • 0: To disable DND and SAC link button. • 1: To enable DND and SAC link button. **Note:** Avaya J159 IP Phone and Avaya J169/J179 IP Phone supports this feature.
APPNAME_IN_USE	Null	Used to check which firmware version is installed on the phone to perform a corresponding action, for example: `IF $APPNAME_IN_USE SEQ 4.0.2.0.11 GOTO CROSSGRADE`
ASTCONFIRMATION	60	Specifies the number of seconds that the phone waits to validate an active subscription when it subscribes to the avaya-cm-feature-status package. Valid values are 16 through 3600.

Table continues…

Parameter name	Default value	Description
AUDASYS	3	Specifies the audible alerting setting for the phone. Value operation: • 0: Turns off audible alerting. User cannot adjust ringer volume. • 1: Turns on audible alerting. User can adjust ringer volume, but cannot turn off audible alerting. • 2: Turns off audible alerting. User can adjust ringer volume and can turn off audible alerting. • 3: Turns on audible alerting. User can adjust ringer volume and can turn off audible alerting. **Note:** Avaya J129 IP Phone does not support this parameter.
AUDIOENV	0	Specifies the audio environment index and enables you to customize the phone's audio performance. Valid values are 0 through299. This parameter affects settings for AGC dynamic range, handset and headset noise reduction thresholds, and headset transmit gain. Always consult Avaya before changing this parameter.
AUDIOPATH	1	Specifies the audio path for the phone. Value operation: • 1: For speaker. • 2: For headset.

Table continues…

Parameter name	Default value	Description
AUDIOPATH_DEFAULT	1234	Specifies the default value of audio path setting in user menu. Value operation: • 1: For speaker. • 2: For headset. • 3: Speaker forced. • 4: Headset forced.
AUDIOSTHD	0	Specifies the level of sidetone in the headset. Value operation: • 0: Normal level for most users • 1: One level softer than normal • 2: Two levels softer than normal • 3: Three levels softer than normal • 4: Off which means inaudible • 5: One level louder than normal
AUDIOSTHS	0	Specifies the level of sidetone in the handset. Value operation: • 0: Normal level for most users • 1: Three levels softer than normal • 2: Inaudible • 3: One level softer than normal • 4: Two levels softer than normal • 5: Four levels softer than normal • 6: Five levels softer than normal • 7: Six levels softer than normal • 8: One level louder than normal • 9: Two levels louder than normal

Table continues…

Parameter name	Default value	Description
AUTH	0	Specifies whether the script files are downloaded from an authenticated server over an HTTPS link. Value operation: • 0: Optional • 1: Mandatory To revert the configured value of 1 to the default one, reset the phone to defaults.
AUTHCTRLSTAT admin	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.
AUTO_SELECT_ANY_IDLE_APPR	0	Specifies that any idle call appearance (primary or bridged) can be automatically selected. This parameter works along with the parameter CONF_TRANS_ON_PRIMARY_APPR. Value operation: • 0: Disabled. Both parameters AUTO_SELECT_ANY_IDLE_APPR and AUTO_SELECT_ANY_IDLE_APPR are set to 0. • 1: Enabled. The parameter CONF_TRANS_ON_PRIMARY_APPR is set to 0.

Table continues…

Parameter name	Default value	Description
AUTO_UNMUTE	0	Specifies whether the call is not in a muted state when the transducer is changed. This feature is applied on all types of calls. Value operation: • 0: Disabled. Call is in mute state. • 1: Enabled. Call is not in mute state.
BACKGROUND_IMAGE	Null	Specifies custom background images that can be loaded from the provisioning server. Phone supports up to 5 background images with the following limitation: • Only jpeg format files are supported. • The maximum file size is 256 KB. • The file names are case sensitive. Example: SET BACKGROUND_IMAGE [xxx.jpg]
BACKGROUND_IMAGE_DISPLAY	Null	Specifies the background image to be displayed on the phone. Value operation: • 0: To select default image 1. • 1: To select default image 2. • 2: To select default image 3. • 3: To select default image 4. • 4: To select default image 5. • 5: To select default image 6. • 6: To select default image 7. Note that, If BACKGROUND_IMAGE_SELECTABLE is set to 1 then the end user may override this setting.

Table continues…

Parameter name	Default value	Description
BACKGROUND_IMAGE_SELECTABLE	1	Allows the end user to select background images. Value operation: • 0: The user can not use a background images from the phone UI. • 1: The user can select a background images from the phone UI.
BACKGROUND_IMAGE_SECONDARY	Null	Specifies a list of background images to be used on the secondary screen. The secondary screen resolution is 240 pixels x 320 pixels and color depth is 16 bits. The image should be jpeg or jpg file with maximum size of 256 KB. The filenames are case insensitive. You can save upto 5 images in the same directory defined by HTTPDIR / TLSDIR. Example: background_example1.jpg,background_example2.jpeg **Note:** This parameter is supported only in Avaya J159 IP Phone
BACKGROUND_IMAGE_DISPLAY_SECONDARY	Null	Specifies the background image to be displayed on the Secondary screen. The filename will be one of the filenames listed in BACKGROUND_IMAGE_SECONDARY. Note that if BACKGROUND_IMAGE_SELECTABLE_SECONDARY is set to 1 then the end user may override this setting.

Table continues…

Parameter name	Default value	Description
BACKGROUND_IMAGE_SELECTABLE_SECONDARY	1	Allows the end user to select background images for the secondary screen. Value operation: • 0: The user can not use a background images from the phone UI. • 1: The user can select a background images from the phone UI. This parameter overrides the value configured using BACKGROUND_IMAGE_DISPLAY_SECONDARY parameter **Note:** This parameter is supported only in Avaya J159 IP Phone
BACKLIGHT_SELECTABLE	0	Specifies whether backlight timer is selected by the administrator (BAKLIGHTOFF) or user. Value operation: • 0: To set Backlight Timer value from `46xxsettings.txt` file. • 1: To set Backlight Timer value according to user settings.
BAKLIGHTOFF	120	Specifies the number of minutes of idle time after which the display backlight will be turned off. Phones with gray-scale displays do not completely turn backlight off, they set it to the lowest non-off level. Valid values are 0 through 999. A value of 0 means that the display backlight will not be turned off automatically when the phone is idle. For ENERGY STAR compliance on applicable phones, a value of 20 is recommended.

Table continues…

Parameter name	Default value	Description
BLOCK_ANONYMOUS_CALLS	0	Specifies that the incoming calls with anonymous details in the **From** header are rejected. Value operation: • 0: Enabled • 1: Disabled
BLOCK_CERTIFICATE_WILDCARDS	0	Specifies whether the endpoint will accept server identity certificates with wildcards. Value operation: • 0: Accept wildcards in certificate. • 1: Do not accept wildcards in certificates.
BLUETOOTHSTAT	1	Specifies whether the user is given an option to enable the Bluetooth. Value operation: • 0: Bluetooth is disabled and the user is not given an option to enable it. • 1: The user is given an option to enable the Bluetooth.
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

Table continues…

Parameter name	Default value	Description
BUTTON_MAPPINGS	Null	Specifies a list of Button and Status pairs that change the operation of some of the buttons on the phone. Button and Status pairs are separated by commas without any intervening spaces. Valid button values are Forward, Speaker, Hookswitch, and Headset. Valid Status values are na and cc-release. Value operation: • na: The corresponding button is disabled. • cc-release: Button invokes the cc-release feature. • null: All buttons operate normally.
C		
CALL_TRANSFER_MODE	0	Determines the call transfer mode in 3rd party environments. Valid value is 0 or 1.
CALLFWDADDR	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	1	Sets the number of ring cycles before the call is forwarded to the forward or coverage address. The default delay is one ring cycle.

Table continues…

Parameter name	Default value	Description
CALLFWDSTAT	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.
CC_INFO_TIMER	8	Specifies the duration, in hours, of the subscription to the SIP CC-Info event package. Valid values are 1 through 24.
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.

Table continues…

Parameter name	Default value	Description
CLDISPCONTENT	1	Specifies whether the name, the number, or both will be displayed for Call Log entries. Value operation: • 0: Both the name and the number will be displayed. • 1: Only the name will be displayed.
CNAPORT	50002	Specifies the TCP destination port used for CNA registration. Valid values are 0 through 65535.
CNASRVR	Null	Specifies a list of CNA server IP addresses. Addresses can be in dotted-decimal (IPv4) or DNS name format, separated by commas without any intervening spaces. The list can contain up to 255 characters. The default value is null.

Table continues…

Parameter name	Default value	Description
CONF_TRANS_ON_PRIMARY_APPR	0	Determines conference and transfer setup whether to use idle primary call appearance or idle bridged call appearance. Value operation: • 0: To specify conference and transfer setup to use an idle primary call appearance at first attempt. However, if an idle primary call appearance is unavailable, then the setup will use idle bridged call appearance regardless of the setting of AUTO_SELECT_ANY_IDLE_APPR. If a bridged call appearance initiates the setup, then setup will use idle bridged call appearance of same extension. If an idle bridged call appearance of the same extension is not available and AUTO_SELECT_ANY_IDLE_APPR is set to 1, then setup will use any idle call appearance. However, if AUTO_SELECT_ANY_IDLE_APPR is set to 0 and if same bidged call extension is not available, the setup initiated on a bridged call appearance will be denied. • 1: To specify conference and transfer setup to use an idle primary call appearance at first attempt. However, if an idle primary call appearance is unavailable, then the setup will use idle bridged call appearance. If a bridged call appearance initiates the setup, then setup will use idle bridged call appearance of either the same extension or different extension. AUTO_SELECT_ANY_IDLE_APPR is ignored.

Table continues…

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

Table continues…

Parameter name	Default value	Description
CONTROLLER_SEARCH_INTERVAL	16	Specifies the number of seconds the phone waits to complete the maintenance check for monitored controllers. Valid values are 4 through 3600.
CONNECTION_REUSE	1	Specifies whether the phone will use two UDP, TCP, or TLS connection (for both outbound and inbound) or one UDP, TCP, or TLS connection. Value operation: • 1: Enabled. The phone does not open a listening socket and will maintain and re-use the sockets it creates with the outbound proxies.
COUNTRY	USA	Used for network call progress tones. • For Argentina use keyword Argentina. • For Australia use keyword Australia. • For Brazil use keyword Brazil. • For Canada use keyword USA. • For France use keyword France. • For Germany use keyword Germany. • For Italy use keyword Italy. • For Ireland use keyword Ireland. • For Mexico use keyword Mexico. • For Spain use keyword Spain. • For United Kingdom use keyword UK. • For United States use keyword USA. Country names with spaces must be enclosed in double quotes.

Table continues…

Parameter name	Default value	Description
COVERAGEADDR	Null	Sets the address to which calls will be forwarded for the call coverage feature. Users can change or replace this administered value if CALLFWDSTAT is not 0.
D		
DATEFORMAT	Null	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.
DES_STAT	2	Specifies if DES discovery is to be attempted during the boot process if there is no configuration file server provisioned on the phone. Value operation: • 0: DES discovery is disabled and can only be restored with Reset to Defaults • 1: DES discovery is disabled • 2: DES discovery is enabled • 3: to set the devices to automatically use DES without the need to select yes on the prompt.

Table continues…

Parameter name	Default value	Description
DHCPSTAT	3	Specifies whether DHCPv4, DHCPv6 or both are used if IPv6 support is enabled by IPV6STAT. **Note:** DHCPv4 is always enabled in IPv4 only and dual mode. DHCPv4 is disabled in IPv6 only mode. Value operation: • 1: run DHCPv4 only. • 2: run DHCPv6 only. • 3: run both DHCPv4 and DHCPv6.
DHCPSTD	0	Specifies whether DHCP complies with the IETF RFC 2131 standard and continues to use the expired DHCP lease. Value operation: • 0: Continue using the address in an extended rebinding state. • 1: Immediately stop using the address.
DHCPSTDV6	0	Specifies whether DHCPv6 will comply with the IETF RFC 8415 standard and immediately stop using an IPv6 address if the address valid lifetime expires, or whether it will enter an extended rebinding state. Value operation: • 0: DHCPv6 enters proprietary extended rebinding state (continue to use IPv6 address, if DHCPv6 lease expires). • 1: DHCPv6 complies with IETF RFC 8415 standard (immediately release IPv6 address, if DHCPv6 lease expires).

Table continues…

Parameter name	Default value	Description
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.
DIR96X1_CONTACT_SOURCE	0	Specifies which contact source will be used to search contacts Value operation: • 0: The default value configured by the administrator • 1: Phone will use search sources configured on the phone • 2: Phone will use LDAP as contact search source.
DIR96X1_CONTACT_SOURCE_DEFAULT	0	Specifies the default directory to be used when a contact search is performed Value operation: • 0: System • 1: LDAP
DIRENABLED_PLATFORM	0	Determines whether the LDAP directory search is enabled on the phone. Value operation: • 0: No • 1: Yes **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
DIRNAME_FIELDS	cn	Specifies the attributes and their order, shown in the search results. Users can view other attributes, pressing the **Details** soft key. T The attributes, specified in this parameter must be a subset of the attributes, specified in DIRNAME_FIELDS. For example, `SET DIRNAME_FIELDS "cn,sn"` In this example, each match on a search result list displays a last name and a first name. **Note:** Avaya J129 IP Phone does not support this parameter.
DIRNUMBER_FIELDS	telephoneNumber	Specifies the LDAP fields that contain a callable number. The first number listed becomes the primary number. For example, `SET DIRNUMBER_FIELDS "telephoneNumber,mobile,DoD SIP URI"` **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
DIRSEARCH_FIELDS	"cn,sn,telephoneNumber"	Specifies LDAP search attributes. The exact number and names of the search attributes depend on the LDAP server configuration and can vary from one LDAP directory to another. When configuring this parameter, you must use attribute names that coincide with the selected LDAP server attribute names. For example, `SET DIRSEARCH_FIELDS "givenName,mail,middle initials, telephoneNumber,sn,mobile ,o , department ,Rank ,office ,DoD SIP URI"` **Note:** Avaya J129 IP Phone does not support this parameter.
DIRSECURE	1	Specifies whether to use TLS or TCP for LDAP. To authenticate the server, startTLS is used. ldaps:// is not supported. You need to configure startTLS for the secure LDAP connection. Value operation: • 0: Use TCP • 1: Use TLS For example, `SET DIRSECURE 1` **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
DIRSHOW_FIELDS	"cn,sn,telephoneNumber,Mail"	Specifies LDAP detail show fields. The phone returns the attributes, specified in this parameter, for each match found for a search query. You can use this parameter to map the specified LDAP keywords. This mapping defines the way the phone displays show fields. For example, `SET DIRSHOW_FIELDS "dn=Distinguished Name, rank, gn=First Name,office=Office,middle initials=Middle Initial,Display Name=Full Name,sn=Last Name,job title=Job,cn=Common Name,o=Office,c=Country,department=Department,street=Street, mail=Mail Box,l,telephoneNumber=PhoneNumber,st,mobile=Mobile,postalCode=Postal code,facsimileTelephoneNumber=Fax,DoD SIP URI=Number"`  In this example, the format is as follows:  `SET DIRSHOW_FIELDS "[LDAP Attributes]=[Field Names], [LDAP Attribute 1]=[Field Name1]"` **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description

DIRSRVR	Null	Specifies the IP address or a fully qualified domain name (FQDN) of the LDAP directory server.
		The valid value is an IPv6, IPv4 address in the dotted decimal format or a FQDN.
		For example,
		`SET DIRSRVR 192.168.161.54`
		or
		`SET DIRSRVR domain.com`
		Note:
		Avaya J129 IP Phone does not support this parameter.

DIRSRVRPRT	636	Specifies the port number for the LDAP directory server. Valid values are positive integers from 1 to 65535. For example, `SET DIRSFVFRT 389` **Note:** Avaya J129 IP Phone does not support this parameter.
DIRTOPDN	Null	Specifies the LDAP search base. For example, `SET DIRTOPDN "dc=global,dc=avaya,dc=com"` **Note:** Avaya J129 IP Phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
DISCOVER_AVAYA_ENVIRONMENT	1	Specifies dynamic feature set discovery Value operation: • 1: The phone discovers and verifies if the controller supports the AST feature set or not. The phone sends a SUBSCRIBE request to the active controller for the Feature Status Event Package (avaya-cm-feature-status). If the request succeeds, the phone proceeds with PPM Synchronization. If the request is rejected, or is proxied back to the phone, or does not receive a response, the phone assumes that AST features are not available. • 0: The phone operates in a mode where AST features are not available. **Note:** Set the parameter to 0 for 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.

Table continues…

Parameter name	Default value	Description
DND_SAC_LINK	0	Specifies whether to activate the SendAllCall when user enables DoNotDisturb The value of this parameter is used if the ALLOW_DND_SAC_LINK_CHANGE is set to 0 Value operation: • 0: Do not activate the SendAllCall when user enables DoNotDisturb (default). • 1: Activate the SendAllCall when user enables DoNotDisturb.
DNSSRVR	Null	Specifies a character string that will be appended to parameter values that are specified as DNS names, before the name is resolved. The value can contain 0 to 255 characters. The default value is null. This parameter can be set through: • DHCP • The settings file. Setting this parameter through the settings file overwrites any values set through DHCP.
DOMAIN	Null	Specifies a character string that will be appended to parameter values that are specified as DNS names, before the name is resolved. The value can contain 0 to 255 characters. The default value is null. This parameter can be set through: • DHCP • The settings file. Setting this parameter through the settings file overwrites any values set through DHCP.

Table continues…

Parameter name	Default value	Description
DOT1X	0	Specifies the 802.1X pass-through operating mode. Pass-through is the forwarding of EAPOL frames between the phone's ethernet line interface and its secondary (PC) ethernet interface Value operation: • 0: EAPOL multicast pass-through enabled without proxy logoff. • 1: EAPOL multicast pass-through enabled with proxy logoff. • 2: EAPOL multicast pass-through disabled.
DOT1XEAPS	MD5	Specifies the authentication method to be used by 802.1X. Valid values are MD5, and TLS.
DOT1XSTAT	0	Specifies the 802.1X supplicant operating mode. Value operation: • 0: Supplicant disabled. • 1: Supplicant enabled, but responds only to received unicast EAPOL messages. • 2: Supplicant enabled; responds to received unicast and multicast EAPOL messages.
DSCPAUD	46	Specifies the layer 3 Differentiated Services (DiffServ) Code Point for audio frames generated by the phone. Valid values are from 0 to 63. This parameter can also be set through the LLDP, which overwrites any value in the settings file.
DSCPAUD_FL	43	Specifies the DSCP value for flash precedence or priority level voice call. Valid values are from 0 to 63.

Table continues…

Parameter name	Default value	Description
DSCPAUD_FO	41	Specifies the DSCP value for flash Override precedence or priority level voice call. Valid values are from 0 to 63.
DSCPAUD_IM	45	Specifies the DSCP value for immediate precedence or priority level voice call. Valid values are from 0 to 63.
DSCPAUD_PR	47	Specifies the DSCP value for priority precedence or priority level voice call. Valid values are from 0 to 63.
DSCPMGMT	16	Specifies the DSCP value for OA&M management packet. Valid values are from 0 to 63.
DSCPSIG	34	Specifies the layer 3 Differentiated Services (DiffServ) Code Point for signaling frames generated by the phone. Valid values are 0 through 63. This parameter can also be set through LLDP, which overwrites any value set in the settings file.
DSTOFFSET	1	Specifies the time offset in hours of daylight savings time from local standard time. Valid values are 0, 1, or 2. The default value is 1.
DSTSTART	2SunMar2L	Specifies when to apply the offset for daylight savings time. The date and time for applying the offset can be set in the following formats: • `odddmmmht`: for example, `2SunMar2L` which corresponds to the second Sunday in March at 2 AM local time; • `Dmmmht`: for example, `10Mar5L` which corresponds to March 10 at 5 AM local time.

Table continues…

Parameter name	Default value	Description
DSTSTOP	1SunNov2L	Specifies when to stop applying the offset for daylight savings time. You can set the date and time when the offset is stopped in the following formats: • `odddmmmht`: for example, `1SunNov2L` which corresponds to the first Sunday in November at 2 AM local time; • `Dmmmht`: for example, `7Nov5L` which corresponds to November 7 at 5 AM local time.
DTMF_PAYLOAD_TYPE	120	Specifies the RTP payload type to be used for RFC 2833 signaling. Valid values are 96 through 127.
DUAL_IPPREF	4	DUAL_IPPREF controls the following: • The selection of SSON either from DHCPv4 or DHCPv6 server, when phone is in dual mode, and • Whether an IPv4 or IPv6 addresses returned by DNS would be tried first during dualmode operation. DHCP clients use DUAL_IPPREF to decide which SSON configuration attributes to apply for DHCPv4 / DHCPv6 interworking in dual mode. Value operation: • 4: IPv4 is preferred. • 6: IPv6 is preferred.
E		
EASG_SITE_AUTH_FACTOR	Null	Specifies Site Authentication Factor code associated with the EASG site certificate being installed. Valid values are 10 to 20 character alphanumeric string.

Table continues…

Parameter name	Default value	Description
EASG_SITE_CERTS	Null	Specifies list of EASG site certificates which are used by technicians when they don't have access to the Avaya network to generate EASG responses for SSH login. The URLs must be separated by commas without any intervening spaces. Valid values are 0 to 255 ASCII characters.
EEESTAT	1	Specifies Energy-Efficient Ethernet (802.3az) is enabled on PHY1 and PHY2. This parameter is supported by only Avaya J129 IP Phone. Value operation: • 0: EEE is disabled on both PHY1 and PHY2. • 1; EEE is enabled on both PHY1 and PHY2.
ELD_SYSNUM	1	Controls whether Enhanced Local Dialing algorithm will be applied for System Numbers-Busy Indicators and Auto Dials. Value operation: • 0: Disable ELD for System Numbers • 1: Enable ELD for System Numbers **Note:** Avaya J139 IP Phone does not support Busy Indicator feature.
ENABLE_3PCC_ENVIRONMENT	1	Specifies that the phone is working in the Third-party call control setup environment. Value operation: • 0: Disabled • 1: Enabled Set the parameter to 0 for Avaya Aura® and IP Office environment.

Table continues…

Parameter name	Default value	Description
ENABLE_AVAYA_ENVIRONMENT	1	Specifies whether the phone is configured to be used in an Avaya (SES) or a third-party proxy environment. Value operation: • 0: Configured for 3rd party proxy with SIPPING 19 features. • 1: Configured for Avaya environment with AST features and PPM.
ENABLE_BLIND_TRANSFER	1	Specifies that whether the blind transfer is enabled or not. Value operation: • 0: Disabled. • 1: Enabled. Avaya J129 IP Phone does not support this feature.
ENABLE_CALL_LOG	1	Species if call logging and associated menus are available on the phone. Value operation: • 0: No • 1: Yes
ENABLE_CONTACTS	1	Specifies if the contacts application and associated menus are available on the phone. Value operation: • 0: No. 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.

Table continues…

Parameter name	Default value	Description
ENABLE_DND	1	Specifies that the do-not-disturb feature is enabled. Value operation: • 0: Disabled • 1: Enabled **Note:** This parameter is only applicable if a 3PCC environment is configured.
ENABLE_DND_PRIORITY_OVER_CFU_CFB	0	Specifies that the Do-not-disturb (DND) feature is given priority over Call forwarding unconditionally (CFU) and Call forwarding busy (CFB). Value operation: • 0: Disabled • 1: Enabled **Note:** This parameter is only applicable if a 3PCC environment is configured.
ENABLE_EARLY_MEDIA	1	Specifies if the phone sets up a voice channel to the called party before the call is answered. Value operation: • 0: No • 1: Yes Setting this parameter to 1 can speed up call setup.
ENABLE_EXCHANGE_REMINDER	0	Specifies whether or not exchange reminders will be displayed. Value operation: • 0: Not displayed • 1: Displayed

Table continues…

Parameter name	Default value	Description
ENABLE_G711A	1	Specifies if the G.711 a-law codec is enabled. Value operation: • 0: Disabled • 1: Enabled
ENABLE_G711U	1	Specifies if the G.711 mu-law codec is enabled. Value operation: • 0: Disabled • 1: Enabled
ENABLE_G722	1	Specifies if the G.722 codec is enabled. Value operation: • 0: Disabled • 1: Enabled
ENABLE_G726	1	Specifies if the G.726 codec is enabled. Value operation: • 0: Disabled • 1: Enabled
ENABLE_G729	1	Specifies if the G.729A codec is enabled. Value operation: • 0: Disabled • 1: Enabled without Annex B support (default). • 2: Enabled with Annex B support.
ENABLE_MLPP	0	Specifies that whether the Multiple Level Precedence and Preemption (MLPP) is enabled or not. Value operation: • 0: Disabled. • 1: Enabled.

Table continues…

Parameter name	Default value	Description
ENABLE_MODIFY_CONTACTS	1	Specifies if the list of contacts and the function of the contacts application can be modified on the phone. Value operation: • 0: No • 1: Yes
ENABLE_MULTIPLE_CONTACT_WARNING	1	Specifies if a warning message must be displayed if there are multiple phones registered on a user's behalf. Value operation: • 0: No • 1: Yes **Note:** Multiple registered phones can lead to service disruption.
ENABLE_OOD_MSG_TLS_ONLY	1	Specifies if an Out-Of-Dialog (OOD) REFER must be received over TLS transport to be accepted. Value operation: • 0: No, TLS is not required. • 1: Yes, TLS is required. **Note:** A value of 0 is only intended for testing purposes.

Table continues…

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

Table continues…

Parameter name	Default value	Description
ENABLE_PUBLIC_CA_CERTS	1	Specifies whether the out-of-the-box phone can validate server certificates against a list of well-known public Certificate Authority certificates Value operation: • 0: Embedded public CA certificates are only trusted when TRUSTCERTS is empty. • 1: Embedded public CA certificates are always trusted.
ENABLE_RECORDING	0	Specifies if audio debug recording is enabled for users. Value operation: • 0: Audio debug recording is disabled. • 1: Audio debug recording is enabled.
ENABLE_REDIAL	1	Specifies if **Redial** softkey is available. Value operation: • 0: No • 1: Yes
ENABLE_REDIAL_LIST	1	Specifies if the phone redials last number or displays list of recently dialed numbers. Value operation: • 0: Last number redial • 1: User can select between the last redialled number and the redial list. • **Note:** Avaya J129 IP Phone and Avaya J139 IP Phone do not support this feature.

Table continues…

Parameter name	Default value	Description
ENABLE_REMOVE_PSTN_ACCESS_PREFIX	0	Allows phone to perform digit manipulation during failure scenarios. This parameter allows removal of PSTN access prefix from the outgoing number. 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.

Table continues…

Parameter name	Default value	Description
ENABLE_SHOW_EMERG_SK_UNREG	2	Specifies whether an **Emergency** softkey, with or without a confirmation screen, is displayed when the phone is not registered. All emergency numbers will always be supported. Value operation: • 0: **Emergency** softkey is not displayed. • 1: **Emergency** softkey is displayed without a confirmation screen. • 2: **Emergency** softkey is displayed with a confirmation screen. **Note:** The parameter is set to 0 for IP Office environment.
ENABLE_SIP_USER_ID	0	Specifies the display of the user ID input field on the Login Screen. Value operation: • 0: Disabled • 1: Enabled
ENABLE_STRICT_USER_VALIDATION	0	Specifies that the validation is done for the **To header** and **Request-URI** against AOR and **Contact** header during phone registration. Value operation: • 0: No validation. • 1: Validates the phone registration.

Table continues…

Parameter name	Default value	Description
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.
ENTRYNAME	0	Specifies if the calling party name, or the VDN or the skill name must be used in **History** entries. Value operation: • 0: Calling Party Name is used. • 1: VDN or the skill name is used.

Table continues…

Parameter name	Default value	Description
EVENT_NOTIFY_AVAYA_MAX_USERS	20	Specifies the maximum number of users to be included in an event notification message from CM/AST-II or Avaya Aura® Conferencing 6.0 or later. Valid values are 0 through 1000. This parameter is used only for development and debugging purposes.
EXCHANGE_AUTH_USERNAME_FORMAT	0	Specifies the necessary format of the username for http authentication. Value operation: • 0: Office 2003/Office2016 username format. Username= <ExchangeUserDomain\ExchangeUserAccount> or Username= <ExchangeUserAccount> if <ExchangeUserDomain> is empty. • 1: Office 365 format. Username= <ExchangeUserAccount@ExchangeUserDomain> or Username= <ExchangeUserAccount> if <ExchangeUserDomain> is empty. **Note:** J159 and J169/179 support this parameter.
EXCHANGE_EMAIL_DOMAIN	Null	Specifies the Exchange email domain. The value can contain 0 to 255 characters. **Note:** J159 and J169/179 support this parameter.

Table continues…

Parameter name	Default value	Description
EXCHANGE_NOTIFY_SUBSCRIPTION_PERIOD	180	Specifies the number of seconds between re-syncs with the Exchange server. Valid values are 0 through 3600. **Note:** J159 and J169/179 support this parameter.
EXCHANGE_REMINDER_TIME	5	Specifies the number of minutes before an appointment at which a reminder will be displayed. Valid values are 0 through 60. **Note:** J159 and J169/179 support this parameter.
EXCHANGE_REMINDER_TONE	1	Specifies whether or not a tone will be generated the first time an Exchange reminder is displayed. Value operation: • 0: Tone not generated. • 1: Tone generated. **Note:** J159 and J169/179 support this parameter.
EXCHANGE_SERVER_LIST	Null	Specifies a list of one or more Exchange server IP addresses. Addresses can be in dotted-decimal or DNS name format, separated by commas without any intervening spaces. The list can contain up to 255 characters. **Note:** J159 and J169/179 support this parameter.

Table continues…

Parameter name	Default value	Description
EXCHANGE_SERVER_SECURE_MODE	1	Specifies if HTTPS should be used to contact Exchange servers. Value operation: • 0: Use HTTP • 1: Use HTTPS **Note:** J159 and J169/179 support this parameter.
EXCHANGE_SNOOZE_TIME	5	Specifies the number of minutes in which a reminder must be displayed again after it is temporarily dismissed. Valid values are 0 through 60. **Note:** J159 and J169/179 support this parameter.
EXCHANGE_USER_DOMAIN	Null	Specifies the domain for the URL used to obtain Exchange contacts and calendar data. The parameter is used as a part of the user authentication. The value can contain 0 to 255 characters. You can change the value by using the Admin menu on the phone. **Note:** J159 and J169/179 support this parameter.
EXTEND_RINGTONE	Null	Provides a way to customize ring tone files. This is a comma separated list of file names in xml format.
F		

Table continues…

Parameter name	Default value	Description
FAILED_SESSION_REMOVAL_TIMER	30	Specifies the number of seconds the phone displays a session line appearance and generates re-order tone after an invalid extension is dialed and user does not press the **End Call** softkey. Valid values are 5 through 999.
FAST_RESPONSE_TIMEOUT	4	Specifies the number of seconds the phone will waits before terminating an INVITE transaction if no response is received. Valid values are 0 through 32. Value of 0 means that this timer is disabled.
FIPS_ENABLED	0	Specifies whether only FIPS-approved cryptographic algorithms will be supported. Value operation: • 0: No restriction on using non FIPS-approved cryptographic algorithms. • 1: Use only FIPS-approved cryptographic algorithms using embedded FIPS 140-2-validated cryptographic module.
FORBIDDEN_SESSION_REMOVAL_TIMER	10	Specifies the duration of an off-hook session before a call automatically ends. This is valid when there are no call appearances available on the called or remote party. Valid values are from 5 to 20 seconds.
FORCE_SIP_EXTENSION	Null	Replaces User ID entered by the user during login.
FORCE_SIP_PASSWORD	Null	Replaces password entered by the user during login.
FORCE_SIP_USERNAME	Null	Replaces the user field entered by the user during login.

Table continues…

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

Table continues…

Parameter name	Default value	Description
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 craft procedure. The default value of GROUP in each phone is 0, and the maximum value is 999.
GUESTDURATION	2	Specifies the duration (in hours) before a Guest Login or a visiting user login is automatically logged off if the phone is idle. Valid values are integers from 1 to 12. **Note:** This parameter is supported by J159 and J169/179 phones.
GUESTLOGINSTAT	0	Specifies whether the Guest Login feature is available to users. Value operation: • 0: The feature is not available. • 1: The feature is availble.. **Note:** This parameter is supported by J159 and J169/179 phones.
GUESTWARNING	5	Specifies the number of minutes, before time specified by GUESTDURATION, that a warning of the automatic logoff is initially presented to the Guest or Visiting User. Valid values are integers from 1 to 15.
H		

Table continues…

Parameter name	Default value	Description
HEADSET_PROFILE_DEFAULT	1	Specifies the number of the default headset audio profile. Valid values are 1 through 20. **Note:** Avaya J129 IP Phonedoes not support this feature.
HEADSET_PROFILE_NAMES	Null	Specifies an ordered list of names to be displayed for headset audio profile selection. The list can contain 0 to 255 UTF-8 characters. Names are separated by commas without any intervening spaces. Two commas in succession indicate a null name, which means that the default name is displayed for the corresponding profile. Names can contain spaces, but if any do, the entire list must be quoted. There is no way to prevent a profile from being displayed. **Note:** Avaya J129 IP Phonedoes not support this feature.
HEADSYS	0	Specifies whether the phone goes on-hook if the headset is active when the disconnect message is received. Value operation: • 0: The phone goes on-hook if the disconnect message is received when the headset is active. • 1: Disconnect messages are ignored when the headset is active. This is used for Call Center setting.

Table continues…

Parameter name	Default value	Description
HOMEIDLETIME	10	Specifies the number of minutes of idle time after which the **Home** screen is displayed. Valid values are 0 through 30. A value of 0 means that the **Home** screen is not displayed automatically when the phone is idle. **Note:** Only Avaya J129 IP Phone supports this feature.
HTTPEXCEPTIONDOMAINS	Null	Specifies a list of one or more domains, separated by commas without any intervening spaces, for which HTTPPROXY is not used. The value can contain 0 to 255 characters. The default value is null.
HTTPPORT	80	Sets the TCP port used for HTTP file downloads from non-Avaya servers. Values range from 0 to 65535.
HTTPPROXY	Null	Specifies the address of the HTTP proxy server used by SIP phones to access an SCEP server that is not on the enterprise network. Valid value can contain zero or one IP address in dotted decimal or DNS name format, optionally followed by a colon and a TCP port number. The value can contain 0 to 255 characters.

Table continues…

Parameter name	Default value	Description
HTTPSRVR	Null	Specifies zero or more HTTP server IP addresses to download configuration script files. The addresses must be separated by commas without any intervening spaces. The format of specifying IP addresses are: • Dotted decimal • Colon-hex • DNS name The parameter can be set by using LLDP. Valid values contains 0 to 255 ASCII characters.
I		
ICMPDU	1	Specifies if ICMP Destination Unreachable messages are generated. Value operation: • 0: No messages are generated. • 1: Limited port unreachable messages are generated. • 2: Protocol and port unreachable messages are generated.
ICMPRED	0	Specifies if received ICMP Redirect messages are processed. Value operation: • 0: No • 1: Yes
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	1	Specifies whether IPv6 will be supported or not. Value operation: • 0: IPv6 will not be supported. • 1: Dual mode. • 2: IPv6 only mode.
K		
L		

Table continues…

Parameter name	Default value	Description
L2Q	0	Specifies if layer 2 frames generated by the telephone have IEEE 802.1Q VLAN tags. Value operation: • 0: Auto. VLAN tagging is turned on when the network can support VLAN tagging and L2QVLAN is non zero. • 1: On. VLAN tagging is turned on when the network can support VLAN tagging. The IP phone sends tagged frames with VLAN = L2QVLAN, even if L2QVLAN is set to 0. • 2: Off. VLAN functionality is disabled. **Note:** This parameter can also be set through: • Local admin procedure • A name equal to value pair in DHCPACK message • SET command in a settings file • DHCP option 43 • LLDP
L2QAUD	6	Specifies the layer 2 priority value for audio frames generated by the telephone. Valid values are 0 through 7. **Note:** This parameter can also be set through: • SET command in a settings file • LLDP. Setting this parameter though LLDP overwrites any values in the settings file.

Table continues…

Parameter name	Default value	Description
L2QSIG	6	Specifies the layer 2 priority value for signaling frames generated by the phone. Valid values are 0 through 7. **Note:** This parameter can also be set through: • SET command in a settings file • LLDP • AADS Setting this parameter through LLDP or AADS overwrites values in the settings file.
L2QVLAN	0	Specifies the voice VLAN ID to be used by IP phones. Valid values are 0 through 4094. **Note:** This parameter can also be set through: • Local admin procedure • A name equal to value pair in DHCPACK message • SET command in a settings file • DHCP option 43 • LLDP
LANGUAGES	Null	Specifies the language files that must be installed or downloaded to the phone. Filenames can be full URL, relative pathname, or filename. Valid values can contain 0 to 1096 ASCII characters, including commas. Filenames must end in `.xml`

Table continues…

Parameter name	Default value	Description
LLDP_ENABLED	2	Specifies whether LLDP is enabled. Value operation: • 0: Disabled • 1: Enabled • 2: Enabled, but only begins transmitting if an LLDP frame is received.
LOCAL_DIAL_AREA_CODE	0	Specifies if user must dial area code for calls within same area code regions. Value operation: • 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.

Table continues…

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

Table continues…

Parameter name	Default value	Description
LOCALLY_ENFORCE_PRIVACY_HEADER The parameter is only available in an Avaya Aura® environment.	0	Specifies whether the phone displays Restricted instead of CallerId information when a Privacy header is received in a SIP INVITE message for an incoming call. Value operation: • 0: Disabled. CallerID information is displayed. • 1: Enabled. Restricted is displayed.
LOG_CATEGORY	Null	Specifies a list of categories of events to be logged through syslog and locally. This parameter must be specified to log events below the Error level. The list can contain up to 255 characters. Category names are separated by commas without any intervening spaces.
LOG_DIALED_DIGITS	1	Specifies if the call log will contain digits dialed by a user or information about a remote party when the user dials a FAC code. The FAC code is identified by * or # entered as a first character. Value operation: • 0: Allow dialed FAC code to be replaced with a remote party number in the call history • 1: Dialed digits are logged in call history exactly as they were entered by the user (default).

Table continues…

Parameter name	Default value	Description
LOGOS		Specifies a list of tuples describing the logo or the wallpaper to be used as the phone display background. Only full path URLs are supported. For 9611G, 9621G and 9641G, the maximum size in pixels are: 217 x 130, 232 x 140 and 232 x 140 respectively with color depth 16 bit and JPG file type. GIF is presented without animation.
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.

Table continues…

Parameter name	Default value	Description
MAX_TRUSTCERTS	10	Specifies the maximum number of trusted certificates files defined by this parameter that can be downloaded to the phone. MAX_TRUSTCERTS enforces the number of certificates. Valid values are from 1 to 10.
MEDIA_ADDR_MODE	4	Specifies the IP address of the endpoint when both IPv4 and IPv6 addresses are provided. This parameter is used for SIP signalling. Value operation: • 4: IPv4 • 6: IPv6 • 46: Prefer IPv4 over IPv6 • 64: Prefer IPv6 over IPv4
MEDIA_NEG_PREFERENCE	0	Specifies the address family preference used by a dual mode answer in non-Avaya environment. This parameter is not applicable for single mode phones. Value operation: • 0: Remote or offerer's preference • 1: Local
MEDIA_PRESERVATION	1	Supports media preservation when ENABLE_IPOFFICE is set to 2. Value operation: • 0: Phone tries to preserve a call for a duration specified by PRESERVED_CALL_DURATION settings parameter. • 1: Phone does not preserve a call. As soon as the phone detects link failure to IP Office, the phone drops a call and makes re-registration attempt.

Table continues…

Parameter name	Default value	Description
MEDIAENCRYPTION	9	Specifies which media encryption (SRTP) options are supported. 3 options can be specified in a comma-separated list. The options must match those specified in Avaya Aura® Communication Manager IP-codec-set form. • 1: aescm128-hmac80 • 2: aescm128-hmac32 • 3: aescm128-hmac80-unauth • 4: aescm128-hmac32-unauth • 5: aescm128-hmac80-unenc • 6: aescm128-hmac32-unenc • 7: aescm128-hmac80-unenc-unauth • 8: aescm128-hmac32-unenc-unauth • 9: none (default) • 10: aescm256-hmac80 • 11: aescm256-hmac32 The list of media encryption options is ordered from high (left) to the low (right) options. The phone 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 (CM) has the capability to change the list order in the SDP-OFFER (for audio only) when it passes through CM. Do not use unauthenticated media encryption (SRTP) files.

Table continues…

Parameter name	Default value	Description
MLPP_MAX_PREC_LEVEL	1	Specifies the maximum allowed precedence level for the user. Value operation: • 1: Routine • 2: Priority • 3: Immediate • 4: Flash • 5: Flash Override
MLPP_NET_DOMAIN	Null	Specifies the MLPP network domain. Value operation: • Null: No domain configured • DSN: DSN network. • UC: UC network.
MP_ENABLED	0	Specifies if the Multicast Paging feature is enabled on the phone. This is the basic parameter for this feature. If this parameter is not set, other parameters listed below will be ignored. Valid values: • 0: Multicast Paging is disabled. • 1: Multicast Paging is enabled.

Table continues…

Parameter name	Default value	Description

MP_GROUPS_TO_LISTEN	Null	Defines the list of Multicast Paging groups that the phone listens to. A maximum of 10 paging groups can be listed.
		
		The paging groups should be separated with a comma (“,”), and should be listed in the following format:
		`IP:port:priority:label`
		
		where
		
		• `IP` is the multicast IP address of an MP group;
		• `Port` is the IP port of a Multicast Paging group, the valid value is an even integer ranging from 1024 to 65534;
		• `Priority` is the priority of a group. Allowed values are 1 through 16, with smaller values indicating a higher priority;
		• `Label` is a group label which is displayed in notification messages when the incoming page from this group is played.
		
		All the above-listed settings are required.
		
		For example,
		`SET MP_GROUPS_TO_LISTEN “239.0.0.0:1208:1:Security,239.1.2.3:1210:4:Sales”`

Table continues…

Parameter name	Default value	Description

MP_GROUPS_TO_SEND	Null	Defines the list of Multicast Paging groups which the phone can send pages to. Priority is not set for these groups. A maximum of 10 paging groups can be listed.
		The paging groups should be separated with a comma (“,”), and should be listed in the following format:
		`IP:port:label`
		`IP`, `Port`, and `Label` denote the same as the corresponding MP_GROUPS_TO_LISTEN values. All these settings are required.
		For example,
		`SET MP_GROUPS_TO_SEND “239.0.0.0:1208:Sales,239.1.2.3:1210:Team”`

MP_CODEC	1	Specifies a codec which will be used to code and decode Multicast Paging transmissions. Valid values: • 1: G.729 codec is used. • 2: G.711u codec is used. • 3: G.711a codec is used.
MP_PACKET_SIZE	20	Specifies the size of an RTP packet in milliseconds. The valid values are 10 through 80. The value must be valid for the selected codec and therefore must not be changed unless necessary.

Table continues…

Parameter name	Default value	Description
MSGNUM	Null	Specifies the phone number to be dialed automatically when the user presses the Message button. The phone number connects to the user's voice mail system. **Note:** This parameter is applicable in Avaya Aura environment. In case of IP Office and third party environment, use the parameter PSTN_VM_NUM.
MUTE_ON_REMOTE_OFF_HOOK	0	Controls the speakerphone muting for a remote-initiated (a shared control or OOD-REFER) speakerphone off-hook. Value operation: • 0: The speakerphone is unmuted. • 1: The speakerphone is muted. The value is applied to the phone only when the phone is deployed with a Avaya Aura® Communication Manager 6.2.2 and earlier releases. If the phone is deployed with Avaya Aura® Communication Manager 6.3 or later, the setting is ignored. Instead the feature is delivered through PPM. The Turn on mute for remote off-hook attempt parameter is enabled in the station form through the Avaya Aura® Session Manageror Avaya Aura® Communication Manager (SAT) administrative interfaces.
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.

Table continues…

Parameter name	Default value	Description
MYCERTCAID	CAIdentifier	Specifies an identifier for the CA certificate with which the SCEP certificate request is to be signed, if the server hosts multiple Certificate Authorities. 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		

Table continues…

Parameter name	Default value	Description
OCSP_ACCEPT_UNK	1	Specifies whether in cases where certificate revocation status for a specific certificate cannot be determined to bypass certificate revocation operation for this certificate. Value operation: • 0: Certificate is considered to be revoked if the certificate revocation status is unknown. TLS connection will be closed. • 1: Certificate revocation operation will accept certificates for which the certificate revocation status is unknown.
OCSP_CACHE_EXPIRY	2880	Specifies the time interval for the OCSP cache expiry in minutes. OCSP response cache expiry uses nextUpdate value in OCSP response message. If nextUpdate is not present, then OCSP_CACHE_EXPIRY parameter value is used. Valid range is from 60 to 10080
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

Table continues…

Parameter name	Default value	Description
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	Null	Specifies a comma separated list of OCSP trusted certificates that are used as OCSP signing authority for checking the revocation status of the certificate. This applies to when the OCSP responder is using a different CA. Spaces are not permitted in this parameter.
OCSP_URI	Null	Specifies the URI of an OCSP responder. The URI can be an IP address or hostname. Valid values contain 0 to 255 ASCII characters, zero or one URI.
OCSP_URI_PREF	1	Specifies the preferred URI for use in an OCSP request when more than one source is available. Value operation: • 1: Use the OCSP_URI and then the OCSP field of the Authority Information Access (AIA) extension of the certificate. • 2: Use the OCSP field of the Authority Information Access (AIA) extension of the certificate and then the OCSP_URI.
OCSP_USE_CACHE	1	Specifies that the OCSP caching is in use. Value operation: • 0: OCSP is not used. Always check with OCSP responder. • 1: OSCP cache caching is used.

Table continues…

Parameter name	Default value	Description
OUTBOUND_SUBSCRIPTION_REQUEST_DURATION	86400	Specifies the duration in seconds requested by the phone in SUBSCRIBE messages, which can be decreased depending on the response from the server. Valid values are 60 through 31536000 (one year). The default value is 86400 (one day).
P		
PHNCC	1	Specifies the country code for United States. The value is 1. Valid values 1 through 999.
PHNDPLENGTH	5	Specifies the internal extension number length. If your extension is 12345, and your dial plan length is 5. The maximum extension length is 13. This value must match the extension length set on your call server. Valid values are 3 through 13.
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, *, #).
PHNIC	011	Specifies the international access code For the United States, the value is 011. Valid values are from 0 to 4 dialable characters (0-9,*,#).

Table continues…

Parameter name	Default value	Description
PHNLAC	Null	Phone's Local Area Code indicates the phone's local area code, which along with the parameter LOCAL_DIAL_AREA_CODE, allows users to dial local numbers with more flexibility. PHNLAC is a string representing the local area code the phone. **Note:** This parameter is supported when the phone is failed over.
PHNLD	1	Specifies the long distance access code Valid values are 0 through 9 and empty string. If long distance access code is not needed then set the parameter to null.
PHNLDLENGTH	10	Specifies the national phone number length. For example, 800-555-1111 has a length of 10. Valid values are 5 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, *, #).

Table continues…

Parameter name	Default value	Description
PHONE_LOCK_IDLETIME	0	Specifies the interval of idle time, in minutes, after which the phone will automatically lock. Valid values are from 0 to 10080. Value operation: • 0: Phone will not lock automatically.
PHY1STAT	1	Specifies the speed and duplex settings for the Ethernet line interface. Value operation: • 1: auto-negotiate • 2: 10Mbps half-duplex • 3: 10Mbps full-duplex • 4: 100Mbps half-duplex • 5: 100Mbps full-duplex • 6: 1Gbps full-duplex, if supported by hardware, otherwise auto-negotiated
PHY2_AUTOMDIX_ENABLED	1	Specifies whether auto-MDIX is enabled on PHY2. Value operation: • 0: auto-MDIX is disabled. • 1: auto-MDIX is enabled.
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. **Note:** J129 does not support this parameter.

Table continues…

Parameter name	Default value	Description
PHY2STAT	1	Specifies the speed and duplex settings for the secondary (PC) Ethernet interface. Value operation: • 0: disabled • 1: auto-negotiate • 2: 10Mbps half-duplex • 3: 10Mbps full-duplex • 4: 100Mbps half-duplex • 5: 100Mbps full-duplex • 6: 1Gbps full-duplex, if supported by hardware, otherwise auto-negotiated
PHY2TAGS	0	Determines whether or not VLAN tags are stripped on Ethernet frames going out of the Computer (PC) port. Value operation: • 0: Strip tags. VLAN tags are stripped from Ethernet frames leaving the computer (PC) port of the phone. • 1: Does not strip tags. VLAN tags are not stripped from Ethernet frames leaving the Computer (PC) port of the phone. **Note:** This parameter is configured through the settings file.

Table continues…

Parameter name	Default value	Description
PHY2VLAN	0	Specifies the value of the 802.1Q VLAN ID used by frames forwarded to and from the secondary (PHY2) Ethernet interface when VLAN separation is enabled. Valid values are 0 through 4094. **Note:** The parameter is configured through the following: • SET command in a settings file • LLDP
PKCS12_PASSWD_RETRY	3	Specifies the number of retries for entering PKCS12 file password. If user failed to enter the correct PKCS12 file password after PKCS12_PASSWD_RETRY retries, then the phone will continue the startup sequence without installation of PKCS12 file. Valid values are from 0 to 100. Value operation: • 0: No retry

Table continues…

Parameter name	Default value	Description
PKCS12URL	Null	Specifies the URL to be used to download a PKCS #12 file containing an identity certificate and its private key. Valid values contain 0 to 255 ASCII characters, zero or one URL. The value can be a string that contains either $SERIALNO or $MACADDR, but it may contain other characters as well. If $MACADDR is added to the URL, then the PKCS12 filename on the file server includes MAC address without colons. PKCS12 file download is preferred over SCEP if PKCS12URL is defined. Value operation: • Null: (Default) Specifies that the PKCS#12 identity certificate download is disabled. • 0 – 255 characters.
PLAY_TONE_UNTIL_RTP	1	Specifies whether locally-generated ringback tone stops as soon as SDP is received for an early media session, or whether it will continue until RTP is actually received from the far-end party. Value operation: • 0: Stop ringback tone as soon as SDP is received. • 1: Continue ringback tone until RTP is received (default).
PRESENCE_ACL_CONFIRM	0	Specifies the handling of a Presence ACL update with pending watchers. Value operation: • 0: Auto confirm. Automatically send a PUBLISH to allow presence monitoring (default). • 1: Ignore. Take no action This parameter is not supported in IP Office environment as presence is not supported.

Table continues…

Parameter name	Default value	Description
PRESENCE_SERVER	Null	Specifies the address of the Presence server. This parameter is supported only for backward compatibility. The value of this parameter is used from PPM and not from the settings file. This parameter is not supported in IP Office environment as presence is not supported.
PRESERVED_CALL_DURATION	120	Specifies the time interval in minutes if ENABLE_IPOFFICE is set to 2 and if MEDIA_PRESERVATION is set to 1. The time interval can be from 10 minutes to 120 minutes.
PRIVACY_SLAAC_MODE	1	Specifies the preference for Privacy Extensions. Value operation: • 0: Disable Privacy Extensions. • 1: Enable Privacy Extensions and prefer public addresses to temporary addresses. • 2: Enable Privacy Extensions and prefer temporary addresses to public addresses.

Table continues…

Parameter name	Default value	Description
PROCPSWD	27238	Specifies an access code to access the local (craft) 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 whether local (craft) procedures can be used to configure the phone. Value operation: • 0: Local procedures can be used (default). • 1: Local procedures cannot be used.
PROVIDE_CF_RINGTONE	0	Specifies if the call forward ringtone option is provided to the user. Value operation: • 0: The call forward ringtone option is not provided (default). • 1: The call forward ringtone option is provided.

Table continues…

Parameter name	Default value	Description
PROVIDE_EXCHANGE_CALENDAR	1	Specifies if menu items for exchange calendar are displayed. Value operation: • 0: Not displayed • 1: Displayed (default) **Note:** Avaya J139 IP Phone does not support Exchange integration feature.
PROVIDE_EXCHANGE_CONTACTS	1	Specifies if menu items for exchange contacts are displayed. Value operation: • 0: Not displayed • 1: Displayed (default) **Note:** Avaya J139 IP Phone does not support Exchange integration feature.

Table continues…

Parameter name	Default value	Description
PROVIDE_KEY_REPEAT_DELAY	0	Specifies how long a navigation button must be held down before it begins to auto-repeat, and if an option is provided by which the user can change this value. Value operation: • 0: Default (500ms) with user option (default). • 1: Short (250ms) with user option. • 2: Long (1000ms) with user option. • 3: Very Long (2000ms) with user option. • 4: No Repeat with user option. • 5: Default (500ms) without user option. • 6: Short (250ms) without user option. • 7: Long (1000ms) without user option. • 8: Very Long (2000ms) without user option. • 9: No Repeat without user option. **Note:** Avaya J129 IP Phonedoes not support this feature.
PROVIDE_LOGOUT	1	Specifies if user can log out from the phone. Value operation: • 0: No • 1: Yes
PROVIDE_NETWORKINFO_SCREEN	1	Specifies if the **Network Information** menu is displayed on the phone. Value operation: • 0: No • 1: Yes

Table continues…

Parameter name	Default value	Description
PROVIDE_OPTIONS_SCREEN	1	Specifies if **Options & Settings** menu is displayed on phone. Value operation: • 0: No • 1: Yes
PSTN_VM_NUM	Null	Specifies the dialable string that is used to call into the messaging system. For example, when you press the **Message Waiting** button. **Note:** This parameter is supported when the phone is failed over.

Table continues…

Parameter name	Default value	Description
PUSHCAP	0000	Controls the modes of individual Push types. The value is a 3, 4 or 5 digit number, of which each digit controls a Push type and can have a value of 0, 1 or 2. Value operation: • 0: all Push requests are rejected for this Push type. • 1: only the Push requests with Barge mode are accepted for this Push type. • 2: the Push requests with Barge or Normal mode are accepted for this Push type. The Push types controlled by each digit (11111) are the following: • ||||+- The rightmost digit controls Top line Push requests. • |||+-- The next digit to the left controls display (WML browser) Push requests. • ||+--- The next digit to the left controls receive audio Push requests. • |+---- The next digit to the left controls transmit audio Push requests. • +----- The next digit to the left controls phonexml Push requests. **Note:** The display Push request (the WML browser) is supported only by the Avaya J169/J179 IP Phone.
PUSHPORT	80	Specifies the TCP port number to be used by the HTTP server in the phone for push. Valid values are 80 through 65535.
Q		

Table continues…

Parameter name	Default value	Description
QLEVEL_MIN	1	Specifies the minimum quality level for which a low local network quality indication will not be displayed. Value operation: • 1: Never display icon (default) • 2: Packet loss is > 5% or round trip network delay is > 720ms or jitter compensation delay is > 160ms. • 3: Packet loss is > 4% or round trip network delay is > 640ms or jitter compensation delay is > 140ms. • 4: Packet loss is > 3% or round trip network delay is > 560ms or jitter compensation delay is > 120ms. • 5: Packet loss is > 2% or round trip network delay is > 480ms or jitter compensation delay is > 100ms. • 6: Packet loss is > 1% or round trip network delay is > 400ms or jitter compensation delay is > 80ms. **Note:** J129 does not support this parameter.

Table continues…

Parameter name	Default value	Description
QTP_BUTTON_COMPRESS	0	Specifies the range of features which can be assigned to Quick Touch Panel on phone screen. Features and Autodials configured on SMGR buttons 4 through 24 will show up on the QTP, up to a maximum of 8 buttons. Call Appearances and Bridged Call Appearances will be excluded from QTP. Value operation: • 0: Buttons will be compressed and all features depicted in SMGR buttons 4 to 11 will be assigned to QTP without blanks. • 1: Buttons will be compressed and blanks removed from the QTP panel. SIP phones do not support call status updates for the softkeys on QTP. The phones do not display any call indication, for example, an incoming call. You must not put call appearances on QTP because the call state display is very limited. To remove Bridged Call Appearances and Call Appearances from QTP, set QTP_BUTTON_COMPRESS to 1.
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.

Table continues…

Parameter name	Default value	Description
RDS_MAX_RETRY_TIME	600	Specifies the maximum delay interval in seconds after which the phone abandons its attempt to contact the PPM server. Valid values are 2 through 3600.
RECORDINGTONE_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.

Table continues…

Parameter name	Default value	Description
RECOVERYREGISTERWAIT	60	Specifies a number of seconds. If no response is received to a REGISTER request within the number of seconds specified by WAIT_FOR_REGISTRATION_TIMER, the phone tries again after a randomly selected delay of 50% to 90% of the value of RECOVERYREGISTERWAIT. Valid values are 10 through 36000.
REDIRECT_TONE	1	Specifies the tone to play when a call goes to coverage. Valid values are from 1 to 4.
REGISTERWAIT	900	Specifies the number of seconds between re-registrations with the current server. Valid values are from 30 to 86400.
REUSETIME	60	Specifies the number of seconds that the DHCP is attempted: • With a VLAN ID of zero. True when L2Q is set to 1. • With untagged frames. True if L2Q is set to 0 or 2. • Before reusing the IP address and the associated address information, that the phone had the last time it successfully registered with a call server. While reusing an address, DHCP enters the extended rebinding state described above for DHCPSTD. Valid values are 0 and 20 through 999. The default value is 60. A value of zero means that DHCP will try forever and there will be no reuse.

Table continues…

Parameter name	Default value	Description
RINGTONES	Null	Specifies a list of display names and file names or URLs for a custom ring tone files to 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.
RINGTONES_UPDATE	0	Specifies if the phone queries the file server to determine if there is an updated version of each custom ring tone file each time the phone starts up or resets. Value operation: • 0: Phone only tries to download ring tones with new display names. • 1: Phone checks for updated version of each ring tone file at startup.
RINGTONESTYLE	0	Specifies the style of ring tones that are offered to the user for personalized ringing when **Classic** is selected, as opposed to **Rich**. Value operation: • 0: North American ring tones are offered (default). • 1: European ring tones are offered.

Table continues…

Parameter name	Default value	Description
RTCP_XR	0	Specifies if VoIP Metrics Report Block as defined in RTP Control Protocol Extended Reports (RTCP XR) (RFC 3611) is sent as part of the RTCP packets to remote peer or to RTCP monitoring server. Value operation: • 0: No • 1: Yes • 2: Sent to RTCP monitoring server only
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.
RTP_PORT_LOW	5,004	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	40	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		

Table continues…

Parameter name	Default value	Description
SCEPPASSWORD	$SERIALNO	Specifies the password to be included in the change password attribute of an SCEP certificate request. Values can contain 0 to 32 ASCII characters (50 ASCII characters. If the value contains `$SERIALNO`, it is replaced by the phone's serial 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. When SCEP_ENTITY_CLASS is set, then SCEPPASSWORD value is set as $SCEP_ENTITY_CLASS:$SCEPPASSWORD, to use it in the enhanced enrollment request.
SCEP_ENTITY_CLASS	Null	Specifies to use the SCEP enrollment request. The value of entity-class is set in SMGR.
SCREENSAVER_IMAGE	N/A	Specifies the screen saver images those can be loaded from the provisioning server. Maximum five custom images can be uploaded onto the phone. Only the .jpeg file format are supported and the maximum file size is 256KB. Note that the image file name is case sensitive.

Table continues…

Parameter name	Default value	Description
SCREENSAVER_IMAGE_DISPLAY	N/A	Allows the administrator to display the desired screen saver image. Note that If BACKGROUND_IMAGE_SELECTABLE is set to 1 then the end user may override this setting.
SCREENSAVER_IMAGE_SELECTABLE	1	Allows the end user to select and change the screen saver images. Value operation: • 0: End user can not select and change the screen saver images from the settings menu. • 1: End user can select and change the screen saver images from the settings menu.
SCREENSAVER_IMAGE_SECONDARY	Null	Specifies a list of screen saver images to be used on the secondary screen. The secondary screen resolution is 240 pixels x 320 pixels and color depth is 16 bits. The image should be jpeg or jpg file with maximum size of 256 KB. The filenames are case insensitive. You can save upto 5 images in the same directory defined by HTTPDIR / TLSDIR. Example: screensaver_example1.jpg, screensaver_example2.jpeg **Note:** This parameter is supported only in Avaya J159 IP Phone

Table continues…

Parameter name	Default value	Description
SCREENSAVER_IMAGE_DISPLAY_SECONDARY	Null	Specifies the screen saver image to be displayed on the Secondary screen. The filename will be one of the filenames listed in SCREENSAVER_IMAGE_SECONDARY. Note that if SCREENSAVER_IMAGE_SELECTABLE_SECONDARY is set to 1 then the end user may override this setting. Example: screensaver_example1.jpg **Note:** This parameter is supported only in Avaya J159 IP Phone
SCREENSAVER_IMAGE_SELECTABLE_SECONDARY	1	Allows the end user to select screensaver images for the secondary screen. Value operation: • 0: The user can not use a screensaver images from the phone UI. • 1: The user can select a background images from the phone UI. This parameter overrides the value configured using SCREENSAVER_IMAGE_DISPLAY_SECONDARY parameter **Note:** This parameter is supported only in Avaya J159 IP Phone

Table continues…

Parameter name	Default value	Description
SCREENSAVERON	240 (4 hours)	Specifies the number of minutes of idle time after which the screen saver is displayed. If an image file is downloaded based on the LOGOS and CURRENT_LOGO parameter, it is used as the screen saver. Otherwise, the built-in Avaya one-X(TM) screen saver is used. Valid values are 0 through 999. The default value is 240 (4 hours). A value of 0 means that the screen saver will not be displayed automatically when the phone is idle.
SDPCAPNEG	1	Specifies if SDP capability negotiation is enabled. Value operation: • 0: SDP capability negotiation is disabled. • 1: SDP capability negotiation is enabled.
SEND_DTMF_TYPE	2	Specifies if DTMF tones are sent in-band as regular audio, or out-of-band using RFC 2833 procedures. Value operation: • 1: In-band • 2: Out-of-band
SERVER_CERT_RECHECK_HOURS	24	Specifies the number of hours after which certificate expiration and OCSP will be used, if OCSP is enabled, to recheck the revocation and expiration status of the certificates that were used to establish a TLS connection. Valid values are from 0 to 32767. Value operation: • 0: Periodic checking is disabled.

Table continues…

Parameter name	Default value	Description
SHORTCUT_ACTION_CONTACT, SHORTCUT_ACTION_AUTODIAL	0	Specifies the action performed if the user presses an Autodial key or selects a contact on the Phone screen during an active call.
SHOW_LAST_EXTENSION	0	Specifies whether to display last extension after logout. Value operation: • 0: To hide last extension after logout. • 1: To display the last extension after logout.
SIG	0	Specifies the type of software to be used by the phone by controlling which upgrade file is requested after a power-up or a reset. Value operation: 0: Download the upgrade file for the same signaling protocol that is supported by the current software (default) 2: Download 96x1Supgrade.txt
SIG_PORT_LOW		Specifies the minimum port value for SIP signaling. (1024 -65503).
SIG_PORT_RANGE		Specifies the range or number of SIP signaling ports. This value is added to SIG_PORT_LOW to determine the upper limit of the SIP signaling port range (32-64511).

Table continues…

Parameter name	Default value	Description
SIGNALING_ADDR_MODE	4	Specifies the SIP controller IP address from SIP_CONTROLLER_LIST_2. This parameter is used by SIP signaling on a dual mode phone. The single IPv4 mode phone ignores SIGNALING_ADDR_MODE and SIP_CONTROLLER_LIST_2 and selects the SIP controller's IP addresses from SIP_CONTROLLER_LIST. The single IPv6 mode phone ignores SIGNALING_ADDR_MODE and SIP_CONTROLLER_LIST and selects the SIP controller's IPv6 addresses from SIP_CONTROLLER_LIST_2. Value operation: • 4: IPv4 • 6: IPv6
SIMULTANEOUS_REGISTRATIONS	3	Specifies the number of Session Managers with which the phone simultaneously register. Valid values are 1, 2 or 3. The default value is 3.

Table continues…

Parameter name	Default value	Description
SIP_CONTROLLER_LIST	Null	Specifies a list of SIP controller designators, separated by commas without any spaces. The list is used on IPv4-only and dual mode phones if SIP_CONTROLLER_LIST_2 is not provided. Controller designator has the following format: `host[:port][;transport=xxx]` where • `host` is an proxy address in dotted-decimal or DNS name format. In third-party call control setup, only DNS format is supported. • `[:port]` is an optional port number. • `[;transport=xxx]` is an optional transport type where `xxx` can be TLS, TCP, or UDP. For example, `SIP_CONTROLLER_LIST="10.138.251.56:5060;transport=tcp"`

Table continues…

Parameter name	Default value	Description
SIP_CONTROLLER_LIST_2	Null	This parameter replaces SIP_CONTROLLER_LIST for dual mode phones. It contains the list of SIP Proxy or Registrar servers separated by comma when the SIP device is configured for the dual-stack operation. SIP_CONTROLLER_LIST_2 is used on IPv6-only phones to provide the list of SIPv6 servers. SIPv4 servers are ignored in IPv6-only mode. Valid values are 0 to 255 characters in the dotted decimal or colon-hex format. The SIP Proxy list has the following format: `host[:port] [;transport=xxx]` where • `host` is IP addresses in dotted-decimal format or hex format. • `[:port]` is the port number. The default values are 5060 for TCP and 5061 for TLS. • `[;transport=xxx]` is the transport type and `xxx` is either TLS or TCP. The default value is TLS. For example, `SIP_CONTROLLER_LIST_2="10.16.26.88:5060;transport=tcp"`
SIP_PORT_SECURE	5061	Specifies the destination TCP port for SIP messages sent over TLS. Valid values are 1024 through 65535. The default value is 5061. The parameter is used in non-Avaya environment. In Avaya environment, this parameter is overwritten by PPM configuration.

Table continues…

Parameter name	Default value	Description
SIPCONFERENCECONTINUE	0	Specifies if a conference call continues after the host hangs up. Value operation: • 0: Drop all parties. • 1: Continue conference **Note:**
SIPDOMAIN	Null	Specifies the domain name to be used during SIP registration. The value can contain 0 to 255 characters. The default value is null.
SIPPORT	5060	Specifies the port the phone opens to receive SIP signaling messages. Valid values are 1024 through 65535. The default value is 5060.
SIPREGPROXYPOLICY	Simultaneous	Specifies if the phone attempts to maintain one or multiple simultaneous registrations. Value operation: • Alternate: Only a single registration is attempted and maintained. • Simultaneous: Simultaneous registrations is attempted and maintained with all available controllers.
SKILLSCREENTIME	5	Specifies the duration, in seconds, that the **Skills** screen is displayed. Valid values are 0 through 60. The default value is 5. A value of 0 means that the **Skills** screen in not removed automatically when the agent logs in.

Table continues…

Parameter name	Default value	Description
SLMCAP	0	Specifies if the SLA Monitor agent is enabled for packet capture. Value operation: • 0: Disabled (default) • 1: Enabled and payloads are removed from RTP packets • 2: Enabled and payloads are included in RTP packets • 3: Controlled from CRAFT menu - Allows you to enable or disable of RTP packets capture using local CRAFT procedures.
SLMCTRL	0	Specifies whether the SLA Monitor agent is enabled for phone control. Value operation: • 0: Disabled • 1: Enabled • 2: Controlled from craft menu.
SLMPERF	0	Specifies whether the SLA Monitor agent is enabled for phone performance monitoring. Value operation: • 0: Disabled • 1: Enabled

Table continues…

Parameter name	Default value	Description
SLMPORT	50011	Specifies the UDP port that will be opened by the SLA Monitor agent to receive discovery and test request messages. Valid values are 6000 through 65535. The default value is 50011. **Note:** If default port is not used, both the SLA Mon agent and the server must be configured with the same port. This parameter impacts the phone's SLA Mon agent configuration. A corresponding configuration must also be made on the SLA Mon server `agentcom-slamon.conf` file.

Table continues…

Parameter name	Default value	Description
SLMSRVR	Null	Specifies the IP address and the port number of the SLA Mon server in the aaa.bbb.ccc.ddd:n format. Set the IP address of the SLA Mon server in the aaa.bbb.ccc.ddd format to restrict the registration of agents only to that server. Specifying a port number is optional. If you do not specify a port number, the system takes 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

Table continues…

Parameter name	Default value	Description
SNMPADD	Null	Specifies a list of source IP addresses from which SNMP query messages will be accepted and processed. Addresses can be in dotted-decimal format (IPv4), colon-hex format (IPv6, if supported), or DNS name format, separated by commas without any intervening spaces. The list can contain up to 255 characters. The default value is null.
SNMPSTRING	Null	Specifies a security string that must be included in SNMP query messages for the query to be processed. Valid values contain 0 through 32 ASCII alphanumeric characters. The default value is null. Null disables SNMP.
SNTP_SYNC_INTERVAL	1440 minutes	Specifies the time interval, in minutes, during which the phone attempts to synchronize its time with configured NTP servers. Valid values are from 60 to 2880 minutes.
SNTPSRVR	Null	Specifies a list of addresses of SNTP servers. Addresses can be in dotted-decimal or DNS name format, separated by commas without any intervening spaces. The list can contain up to 255 characters.
SOFTKEY_ACTIVE_PAGETARGET		Specifies new custom softkey for Call Appearance lines in ACTIVE PAGE state

Table continues…

Parameter name	Default value	Description
SOFTKEY_CONFIGURATION	0,1,2	Specifies which feature will show up on which softkey on the Avaya J129 IP Phonescreens. The features are defined as follows: • 0 = Redial • 1 = Contacts • 2 = Emergency • 3 = Recents • 4 = Voicemail
SP_DIRSRVRPORT	389	Sets the TCP port number of the LDAP Directory Server. The default port number is 389.
SP_DIRTOPDN	Null	Sets the Directory Topmost Distinguished Name. This value must be set to a non-null value to enable the LDAP application. The default is null, but DIRTOPDN should be set to the LDAP root entry.
SPEAKERSTAT	2	Specifies the operation of the speakerphone. Value operation: • 0: Speakerphone disabled • 1: One-way speaker (also called monitor) enabled. • 2: Full (two-way) speakerphone enabled. **Note:** This parameter is not supported on Avaya J129 IP Phone.

Table continues…

Parameter name	Default value	Description
SSH_ALLOWED	2	Specifies if SSH is supported. Value operation: • 0: Disabled • 1: Enabled • 2: Configured using local craft procedure. When this mode is configured, then by default the SSH server is disabled.
SSH_BANNER_FILE	Null	Specifies the file name or URL for a custom SSH banner file. If the value is null, english banner is used for SSH. The value can contain 0 to 255 characters.
SSH_IDLE_TIMEOUT	10	Specifies the idle time in minutes after which an SSH connection is terminated Valid values are 0 through 32767. A value of 0 means that the connection will not be terminated.
SUBSCRIBE_SECURITY	0	Specifies the use of SIP or SIPS for subscriptions. Value operation: • 0: The phone uses SIP for both the request URI and the contactheader regardless of whether SRTP is enabled. • 1: The phone uses SIPS for both the request URI and the contact header if SRTP is enabled. TLS is on and MEDIAENCRYPTION has at least one valid crypto suite. • 2: SES or PPM does not show a FS-phoneData FeatureName with a Feature Version of 2 in the response to the getHomeCapabilities request. For IP office environment, the applicable values are 0 and 1.

Table continues…

Parameter name	Default value	Description
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.
SYSLOG_ENABLED	0	Specifies if sending Syslog messages is enabled or not. Value operation: • 0: Sending Syslog messages is disabled. • 1: Sending Syslog messages is enabled. **Note:** The phone does not display the Secure call icon, if you set the parameter value to 1.

Table continues…

Parameter name	Default value	Description
SYSLOG_LEVEL	4	Specifies the severity level of syslog messages. Events with the selected severity level and above will be logged. the lower numeric severity values correspond to higher severity levels. Value operation: • 3: Error, Critical, Alert and Emergency events are logged • 4: Warning, Error, Critical, Alert and Emergency events are logged (Default) • 5: Notice, Warning, Error, Critical, Alert and Emergency events are logged • 6: Informational, Notice, Warning, Error, Critical, Alert and Emergency events are logged. • 7: Debug, Informational, Notice, Warning, Error, Critical, Alert and Emergency events are logged.
SYSTEM_LANGUAGE	Mlf_English.xml	Contains the name of the default system language file used in the phone. The filename should be one of the files listed in the LANGUAGES parameter. If no filename is specified, or if the filename does not match one of the LANGUAGES values, the phone uses the built-in English text strings. Valid values range from 0 through 32 ASCII characters. Filename must end in .xml
T		
TCP_KEEP_ALIVE_INTERVAL	10	Specifies the number of seconds that the telephone waits before re-transmitting a TCP keep-alive (TCP ACK) message. Valid values are from 5 through 60.

Table continues…

Parameter name	Default value	Description
TCP_KEEP_ALIVE_STATUS	1	Specifies if the phone sends TCP keep alive messages. Value operation: • 0: Keep-alive messages are not sent. • 1: Keep-alive messages are sent (default).
TCP_KEEP_ALIVE_TIME	60	Specifies the number of seconds that the telephone waits before sending out a TCP keep-alive (TCP ACK) message. Valid values are from 10 through 3600
TEAM_BUTTON_REDIRECT_INDICATION	0	Specifies if the redirection indication must be shown on a team button on the monitored station, if it is not a redirect destination of the monitored station. Value operation: • 0: Disabled. The redirect indication is shown only on a monitoring station which is redirection destination. • 1: Enabled. The redirection indication is displayed on all monitoring stations. **Note:** Avaya J129 IP Phoneand Avaya J139 IP Phone do not support this feature.
TEAM_BUTTON_RING_TYPE	1	Specifies the alerting pattern to use for team buttons. Valid values are 1 through 8. The default value is 1. **Note:** Avaya J129 IP Phoneand Avaya J139 IP Phone do not support Team Button feature.

Table continues…

Parameter name	Default value	Description
TIMEFORMAT	0	Specifies the format for time displayed in the phone. The TIMEFORMAT parameter is used when the phone fails to get time format from the PPM. Value operation: • 0: AM or PM format. • 1: 24 hour format
TLS_VERSION	0	Specifies the TLS version used for all TLS connections (except SLA monitor agent) Value operation: 0: TLS versions 1.0 and 1.2 are supported. 1: TLS version 1.2 only is supported.
TLSDIR	Null	Specifies the HTTPS Server Directory Path. Valid values can contain 0 to 127 ASCII characters, without any spaces.
TLSPORT	443	Specifies the TCP port used for HTTPS file downloads from non-Avaya servers. Valid values are from 0 to 65535.
TLSSRVR	Null	Specifies zero or more HTTPS server IP addresses, which is used to download configuration script files. The IP addresses can be specified in dotted-decimal, or DNS name format separated by commas without any intervening spaces. Valid values contain 0 to 255 ASCII characters, including commas. This parameter can also be changed through LLDP.

Table continues…

Parameter name	Default value	Description
TLSSRVRID	1	Specifies how a phone evaluates a certificate trust. Value operation: • 0: Identity matching is not performed. • 1: The certificate is trusted only if the identity used to connect to the server matches the certificate identity, as per Section 3.1 of RFC 2818. For SIP-TLS connections, an additional check is performed to validate the SIP domain identified in the certificate, as per RFC 5922. The parameter is configured through the `46xxsettings.txt` file.
TPSLIST	Null	Specifies a list of URI authority components (optionally, including scheme and path components) to be trusted. A URI received in a push request is only used to obtain push content, if it matches one of these values. The list can contain up to 255 characters. Values are separated by commas without any intervening spaces. If the value of TPSLIST is null, push is disabled.
TRUSTCERTS	Null	Specifies a list of names of files that contain copies of CA certificates (in PEM format) that are downloaded, saved in non-volatile memory, and used by the telephone to authenticate received identity certificates. The list can contain up to 255 characters. ## Values are separated by commas without intervening spaces.
U		

Table continues…

Parameter name	Default value	Description
USE_CONTACT_IN_REFERTO	1	Specifies which transfer target address should be used in Refer-To a header of REFER SIP request on attended transfer. Value operation: • 0: Use CONTACT URI of the transfer target in Refer-To header of REFER SIP request. • 1: Use TO URI of the transfer target in Refer-To header of REFER SIP request.
USE_EXCHANGE_CALENDAR	0	Specifies whether the Calendar synchronizes with the Microsoft Exchange. Value operation: • 0: To disable synchronization. • 1: To enable synchronization.
USE_QUAD_ZEROES_FOR_HOLD	0	Specifies how Hold will be signaled in SDP. Value operation: • 0: “a=directional attributes" will be used • 1: "c=0.0.0.0" will be used
UUIDISPLAYTIME	10	Specifies the duration, in seconds, that the **UUI Information** screen is be displayed. Valid values are 5 through 60.
V		

Table continues…

Parameter name	Default value	Description
VLANSEP	0	Specifies whether VLAN separation is enabled by the built-in Ethernet switch while the phone is tagging frames with a non-zero VLAN ID. When VLAN separation is enabled, only frames with a VLAN ID that is the same to the VLAN ID used by the phone (as well as priority-tagged and untagged frames) is forwarded to the phone. Also, if the value of PHY2VLAN is non-zero, only frames with a VLAN ID that is the same to the value of PHY2VLAN (as well as priority-tagged and untagged frames) is forwarded to the secondary (PHY2) Ethernet interface. Tagged frames received on the secondary Ethernet interface will have their VLAN ID changed to the value of PHY2VLAN and their priority value changed to the value of PHY2PRIO. Value operation: 0: Disabled. 1: Enabled if L2Q, L2QVLAN and PHY2VLAN are set appropriately (default). **Note:** J129 phone does not support this parameter.

Table continues…

Parameter name	Default value	Description
VLANSEPMODE	0 1 for J129	Specifies whether full VLAN separation is be enabled by the built-in Ethernet switch while the telephone is tagging frames with a non-zero VLAN ID. This VLAN separation is enabled when: VLANSEP=1, L2QVLAN and PHY2VLAN have non-zero values, L2Q is auto (0) or (1) tagging.PHY2PRIO is not supported when VLANSEPMODE is 1. Value operation: • 0: Disabled • 1: Enabled **Note:** This parameter is configured through the settings file.
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

Table continues…

Parameter name	Default value	Description
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_CALL_OPERATION_RESPONSE	3	Specifies the time in seconds before providing the user a notification that there is a call operation in progress. This parameter is applicable to all server environments. Example: User goes off-hook, the phone sends an invite. If there is no response from the proxy for three (default value) seconds, the phone will display the notification. Valid values range from 0 to 4. • 0: the notification is disabled • 1 – 4: the number of seconds before the popup display
WAIT_FOR_INVITE_RESPONSE_TIMEOUT	60	Specifies the maximum number of seconds that the phone waits for another response after receiving a SIP 100 Trying response. Valid values are 30 through 180.
WAIT_FOR_REGISTRATION_TIMER	32	Specifies the number of seconds that the phone waits for a response to a REGISTER request. If no response message is received within this time, registration will be retried based on the value of RECOVERYREGISTERWAIT. Valid values are 4 through 3600.

Table continues…

Parameter name	Default value	Description
WAIT_FOR_UNREGISTRATION_TIMER	32	Specifies the number of seconds the phone waits before assuming that an un-registration request is complete. Un-registration includes termination of registration and all active dialogs. Valid values are 4 through 3600.
WARNING_FILE	Null	Specifies the file name or URL for a custom single-channel WAV file coded in ITU-T G.711 u-law or A-law PCM with 8-bit samples at 8kHz to be used as a call recording warning instead of the built-in English warning. The value can contain 0 to 255 characters.
WBCSTAT	1	Specifies whether a wideband codec indication is displayed when a wideband codec is used. Value operation: • 0: Disabled • 1: Enabled **Note:** J129 does not support this parameter

Table continues…

Parameter name	Default value	Description
WEB_ADMIN_PASSWORD	27238	Specifies the password to access the phone through a web browser as an administrator. The value set from the web server interface has a higher priority than that of the Settings file. If the Web admin password is changed using the web server, then the web admin password set through settings file is not used until either the web admin password is set to default through the phone admin menu or the phone is reset to default. Valid values are from 8 to 31 alphanumeric characters including upper, lower and special characters.
WEB_HTTP_PORT	80	Specifies the port on which the Web Server running on the phone will be accessed using HTTP. Valid values are 0, 80, 1024 to 65535.
WEB_HTTPS_PORT	443	Specifies the port on which the Web Server running on the phone will be accessed using HTTPS. Valid values are 443, 1024 to 65535.
WEBSERVER_ON_HTTP	0	Specifies whether HTTP access to the web server is enabled or disabled. Value operation: • 0: Web Server is not accessible through HTTP. • 1: Web Server is accessible through HTTP.
WLAN_MAX_AUTH_FAIL_RETRIES	3	Specifies the number of times the phone will retry a secure connection upon receiving (possibly successive) auth failures. The valid values range from 0 to 4.

Table continues…

Parameter name	Default value	Description
WMLEXCEPT	Null	Specifies zero or more IP addresses or domains for which the HTTP proxy server specified by WMLPROXY will not be used. The values are separated by commas without any intervening spaces. The value can contain up to 255 characters. Only Avaya J169/J179 IP Phones support this parameter.
WMLHOME	Null	Specifies the URL of a WML page to be displayed by default in the WML browser and if the **Home** softkey is selected in the browser. The allowed value contains not more than one URL of up to 255 characters. Only Avaya J169/J179 IP Phones support this parameter. **Note:** If the value is set to default, the WML browser is disabled.
WMLIDLETIME	10	Specifies the idle time in minutes after which the web page set as the value of WMLIDLEURI will be displayed. The allowed value is a positive integer from 1 to 999. Only Avaya J169/J179 IP Phones support this parameter. **Note:** If WMLIDLEURI is set to null, the web page will not be displayed when the phone is idle.

Table continues…

Parameter name	Default value	Description
WMLIDLEURI	Null	Specifies the URL for a WML page to be displayed when the telephone has been idle for the time interval in minutes specified by the WMLIDLETIME parameter. The allowed value contains not more than one URL of up to 255 characters. Only Avaya J169/J179 IP Phones support this parameter.
WMLPORT	8080	Specifies the TCP port number of the HTTP proxy server set as the WMLPROXY value. Allowed values are from 0 to 65535. Only Avaya J169/J179 IP Phones support this parameter.
WMLPROXY	Null	Specifies the IP addresses or domains for which the HTTP proxy server set as the WMLPROXY value will not be used. Allowed values can contain up to 255 characters and must be separated by commas without any intervening spaces. Only Avaya J169/J179 IP Phones support this parameter.

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W