Installing and Maintaining Avaya 9601/9608/9608G/9611G/9621G/9641G/ 9641GS IP Deskphones SIP

Release 7.0.1.2
August 2016

Note

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

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

Heritage Nortel Software

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the

documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

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 G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Regulatory Statements

Australia Statements

Handset Magnets Statement:

Danger:

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

Industry Canada (IC) Statements

RSS Standards Statement

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. L'appareil ne doit pas produire de brouillage, et
2. L'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Radio Transmitter Statement

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

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

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

Radiation Exposure Statement

This device complies with Industry Canada's RF radiation exposure limits set forth for the general population (uncontrolled environment) and must not be co-located or operated in conjunction with any other antenna or transmitter.

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

Japan Statements

Class B Statement

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

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

Denan Power Cord Statement

Danger:

Please be careful of the following while installing the equipment:

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

警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

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

México Statement

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

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

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

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

Power over Ethernet (PoE) Statement

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

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.

802.11b/802.11g/BT 警語：

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.

Class B Part 15 Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designated to provide reasonable protection against harmful interferences in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interferences to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment . This equipment should be installed and operated with minimum distance of 8 in or 20 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

EU Countries

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

General Safety Warning

- Use only the Avaya approved Limited Power Source power supplies specified for this product.
- There is a risk of explosion if you use an incorrect type of battery in the DECT handset. Replace used batteries with the correct battery type: Nickel Metal Hydride (NiMH), rechargeable, size AAA.
  - This product uses NiMH batteries which are recyclable and must not be disposed of as municipal waste to reduce the risk of releasing substances into the environment. At the end of the battery's useful life, remove the rechargeable batteries and take them to the nearest battery collection location to be recycled.
- Ensure that you:
  - Do not operate the device near water.
  - Do not use the device during a lightning storm.
  - Do not report a gas leak while in the vicinity of the leak.
  - Limit the power to the device over telecommunications wiring to 36-57 volt DC or ≤ 1.3 ampere DC.

To ensure the EMC Class B compliance when using a Collaboration Station with an external HDMI monitor, the monitor must be of a type with an external AC or DC power supply.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

This document contains information about preparing for 9600 Series IP Deskphones installation, deployment, initial administration, maintenance and troubleshooting. This document covers administration information for only the following 9600 Series IP Deskphones models:

- 9601
- 9608
- 9608G
- 9611G
- 9621G
- 9641G
- 9641GS

This document is intended for people who install and maintain the 9600 Series IP Deskphones.

Chapter 2: Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP overview

9600 Series IP Deskphones overview

9600 Series IP Deskphones is a series of desk handset devices that you can use for unified communication. The series leverages the enterprise IP network and eliminates the need for a separate voice network.

Avaya 9600 Series IP Deskphones offers high audio quality and customizability with low power requirements. With the high-performance models of this series that can operate in both the H.323 and the Session Initiated Protocol (SIP) environment, you can:

- Make conference calls more efficient and enhance customer interactions with high-quality audio.
- Gain access to information quickly through easy-to-read and high-resolution displays.
- Speed 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 using efficient Power-over-Ethernet (POE) including sleep mode which lowers energy consumption dramatically.

The 9600 Series IP Deskphones works with the Avaya Aura® environment to provide a flexible architecture that works with your investments and accommodates growth as your business needs change.

Related links

9600 Series IP Deskphones models on page 10

9600 Series IP Deskphones models

Deskphone model	Description
9601	The 9601 deskphone is SIP-only phone that provides a four-row monochrome display and two lines with dual red and green LEDs. The phone has a built in 10/100 Ethernet switch with a port for your personal computer or a laptop.
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.

Related links

9600 Series IP Deskphones overview on page 9

New in this release

General enhancements

- Improved upgrade process for the deskphones

Administrative features

- Introduced Hunt group busy button to start or stop receiving calls for the hunt group.

Chapter 3: Initial setup and connectivity

Installation checklist

Use the following checklist to see the tasks that you must perform to install 9600 Series IP Deskphones.

No.	Task	Reference	✔
1.	Check the prerequisites	See Prerequisites on page 11	
2.	Gather preinstallation data	See Preinstallation data gathering on page 12	
3.	Configure the servers	See Server configurations on page 14	
4.	Configure the settings file	See Configuring the settings file on page 17	
5.	Create users on Avaya Aura® System Manager	See Creating users on System Manager on page 20	
6.	Plugging the 9600 Series IP Deskphones to the power source.	See Plugging in the deskphone on page 21.	

Prerequisites

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

Related links

Software requirements on page 11

Hardware requirements on page 12

Software requirements

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

- Avaya Aura® Session Manager 6.3.8 or later
- Avaya Aura® Communication Manager 6.3.6 or later

- Avaya Aura® System Manager 6.3.8 or later
- Avaya Aura® Presence Services 6.2.4 or later
- Avaya Aura® Session Border Controller 7.0 and 7.0.1
- IP Office 10.0 or later
- A DHCP server for providing dynamic IP addresses to the 9600 Series IP Deskphones.
- A file server, an HTTP, HTTPS, or the Avaya Aura® Utility Services for downloading the software distribution package and the settings file

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

Related links

Prerequisites on page 11

Hardware requirements

Ensure that the LAN:

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

Related links

Prerequisites on page 11

Preinstallation data gathering

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

Data for	Field	Value	Notes
System Manager User Profile			
Identity tab			
	First Name		
	Login Name		
	Password		
	Localized Display Name		
	Endpoint Display Name		

Table continues…

Data for	Field	Value	Notes
	Language Preference		
	Time Zone		
Communication Profile tab			
Communication Profile section			
	Communication Profile Password		
Communication Address section			
	Handle Types are for: • Avaya SIP • Avaya E.164 • Avaya Presence/IM if Presence is used		
	Handle Fully Qualified Address		
Session Manager Profile section			
	Primary Session manager		
	Secondary Session Manager		
	Origination Application Sequence		
	Termination Application Sequence		
	Survivability Server		
	Home Location		
CM Endpoint Profile section			
	System		
	Profile Type		
	Use Existing Endpoints		
	Extension		
	Endpoint Template		
	Voice Mail Number		

Table continues…

Data for	Field	Value	Notes
Messaging Profile section			Optional
	System		
	Mailbox Number		
	Template		
	Password		
	Delete Subscriber on Unassign and Delete		
DHCP settings			For dynamically assigning IP addresses to the deskphones and any initial configuration that is required through DHCP options.
	Range of IP addresses		
	DHCP options		
SIP settings			For registering deskphones.
	SIP controller list		
	SIP domain		
File server address			To download the software distribution package and the settings file.
	• HTTPSRVR or TLSSRVR		

Server configuration

To install the 9600 Series IP Deskphones, you need to configure the following servers:

- DHCP server: To dynamically assign IP addresses to the 9600 Series IP Deskphones and, if required, provide the device configuration parameters.
- HTTP or HTTPS server: To download and save the software distribution package and the settings file.

Related links

DHCP server configuration on page 15
File server configuration on page 15

DHCP server configuration

Configure the DHCP server to:

- Dynamically assign IP addresses to the 9600 Series IP Deskphones.
- Provision device and site-specific configuration parameters through various DHCP options.

For more information about the device and site-specific configuration parameters, see *Administering Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP*.

Related links

Server configuration on page 14
Setting up a DHCP server on page 15

Setting up a DHCP server

Procedure

1. Install the DHCP server software according to the vendor instructions.
2. Configure the range of IP address available to the 9600 Series IP Deskphones.
3. Configure the required DHCP options.

Related links

DHCP server configuration on page 15

File server configuration

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

On restarting, the deskphone checks for software updates and settings files on the specified file servers.

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

- DHCP
- LLDP
- Device interface
- Settings file

Related links

Server configuration on page 14
Software distribution package on page 16
Setting up a file server on page 16
Downloading and saving the software on page 16

Software distribution package

The software distribution package includes:

- Signed Software Package files
- An upgrade file named `96x1Supgrade.txt`
- A file named `av_prca_pem_2033.txt` that contains a copy of the Avaya Product Root Certificate Authority certificate in PEM format
- A file named `av_sipca_pem_2027.txt` that contains a copy of the Avaya SIP Root Certificate Authority certificate in PEM format
- A file named `release.xml` that is used by the Avaya Software Update Manager application
- A directory named `signatures` that contains signature files and a Signing Authority Certificate file named `RootSA.txt`
- Language files

Related links

File server configuration on page 15

Setting up a file 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.

Related links

File server configuration on page 15

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 `9600 Series IP Deskphones`.
3. In the **Choose Release** field, click the required release number.
4. Click the **Downloads** tab.

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

The system displays the Downloads page.

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

   The system displays the Downloads page.

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

Related links

File server configuration on page 15

Configuring the settings file

About this task

Modify the settings file with appropriate values to provision the device configuration parameters.

Procedure

1. On the file server, go to the location where you downloaded the settings file.
2. Open the settings file in a text editor.
3. Set the required parameters.
4. Save the settings file.

Related links

Configuration of initial parameters on page 17

Configuration of initial parameters

Set the following initial parameters in the settings file. For more information and a complete list of the settings file parameters, see *Administering Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP*.

Conferencing

Set the following parameter to enable Avaya Aura® Conferencing.

Parameter	Type	Default value	Description
CONFERENCE_FACTORY_URI	String	Null	Specifies the conference server URI used to start an Avaya Aura® Conferencing conference call.

Avaya Aura® Presence Services

Set the following parameter to enable the Avaya Aura® Presence Servicesservices.

Parameter	Type	Default value	Description
PRESENCE_SERVER	String	Null	Specifies the IP address of the Avaya Aura® Presence Servicesserver. The range is from 0 to 255 characters.

SIP registration

Set the following parameters to provide SIP registration information to the device.

Parameter	Type	Default value	Description
SIP_CONTROLLER_LIST	String	Null	Specifies a comma separated list of IP addresses of SIP proxy or registrar server. The range is from 0 to 255. The list has the following format. host[:port][;transport=xxx], where: • host is an IP address in dotted-decimal format • port is the optional port number. If you do not specify a port number, the system uses the following default values: - 5060 for UDP and TCP - 5061 for TLS • transport is the optional transport type, tls, tcp, or udp. If you do not specify the transport, the system uses TLS as the default type For example, `SET SIP_CONTROLLER_LIST proxy1,proxy2:5060;transport=tcp`
CONFIG_SERVER	String	Null	Specifies the address of the PPM configuration server. If the SIP environment it set up such that the PPM server is at a different location than the SIP proxy server address, the device uses the configuration server address instead. The device will not use the proxy server for PPM.
SIPDOMAIN	String	Null	Specifies the SIP domain name for registration. The range is from 0 to 255.

Time settings

Set appropriate network time protocol server and time zone offset as the user does not have the ability to manually set the clock on the device.

Parameter	Type	Default value	Description
SNTPSRVR	String	Null	Specifies a list of zero or more SNTP servers IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces. The range is from 0 to 255 characters.
GMTOFFSET	String	0:00	Specifies offset from Greenwich Mean Time. A positive or negative number of hours and minutes less than 13 hours, 1 to 6 characters, optionally beginning with a plus (+) or minus (-) followed by one or two number digits whose combined value is from 0 to 12 optionally followed by a colon (:) and two numeric digits whose combined value is from 00 to 59.
DSTOFFSET	Numeric	1	Specifies the daylight Saving Time offset from local time.
DSTSTART	String	2SunMar2L	Specifies the Daylight Saving Time start date. Use one of the following formats: • odddmmmht • Dmmmht where, • o is 1 character representing an ordinal adjective as follows: “1” (first), “2” (second), “3” (third), “4” (fourth) or “L” (last) • ddd is 3 characters containing the English abbreviation for the day of the week as follows: “Sun”, “Mon”, “Tue”, “Wed”, “Thu”, “Fri” or “Sat” • mmm is 3 characters containing the English abbreviation for the month as follows: “Jan”, “Feb”, “Mar”, “Apr”, “May”, “Jun”, “Jul”, “Aug”, “Sep”, “Oct”, “Nov” or “Dec” • h is 1 numeric digit representing the time at which to make the adjustment, exactly on the hour at hAM (0h00 in military format), where valid values of h are "0" through "9" • t is 1 character representing the time zone relative to which to make the adjustment as follows: “L” (local time) or “U” (universal time) • D is is 1 or 2 ASCII digits representing the date of the month, from “1” or “01” to “31”, or the character “L”, which means the last day of the month
DSTSTOP	String	1SunNov2L	Specifies the Daylight Saving Time stop date. The following options are applicable: • odddmmmht • Dmmmht

Table continues…

Parameter	Type	Default value	Description
			where, • o is 1 character representing an ordinal adjective as follows: “1” (first), “2” (second), “3” (third), “4” (fourth) or “L” (last). • ddd is 3 characters containing the English abbreviation for the day of the week as follows: “Sun”, “Mon”, “Tue”, “Wed”, “Thu”, “Fri” or “Sat”. • mmm is 3 characters containing the English abbreviation for the month as follows: “Jan”, “Feb”, “Mar”, “Apr”, “May”, “Jun”, “Jul”, “Aug”, “Sep”, “Oct”, “Nov” or “Dec”. • h is s 1 numeric digit representing the time at which to make the adjustment, exactly on the hour at hAM (0h00 in military format), where valid values of h are "0" through "9" . • t is 1 character representing the time zone relative to which to make the adjustment as follows: “L” (local time) or “U” (universal time). • D is is 1 or 2 ASCII digits representing the date of the month, from “1” or “01” to “31”, or the character “L”, which means the last day of the month.

Microsoft Exchange server account settings

Configure the following parameters to setup the Microsoft Exchange Server account for an user:

Related links

Configuring the settings file on page 17

Creating users on Avaya Aura® System Manager

Procedure

1. In a Web browser, enter the System Manager IP address and click **Enter**.
2. Log in to the application with your credentials.
3. Click **User Management** > **Manage Users**.
4. Click **New**.
5. On the **Identity** tab, enter the user details.
6. Click the **Communication Profile** tab.
7. Enter details for Communication Address, Session Manager Profile, CM Endpoint Profile, and Messaging Profile sections.

The phone type must be 9608SIP, 9611SIP, 9621SIP, or 9641SIP so that the default template is used. Use 9608SIP while installing a 9601 SIP Deskphone.

8. Click **Commit & Continue**.

Plugging in the deskphone

About this task

Caution:

Use the correct jack when you plug in the deskphone. You can find the jacks at the rear of the deskphone housing. Icons on the side of the jacks represent the correct use of each jack.

You can only provide power to the 9608, 9608G, 9611G, 9621G, 9641G and 9641GS deskphones with the IP Phone Global Single Port PoE Injector (GSPPOE-xx), the new Telephone Power Module (DC power jack) which is available separately (Comcode 700511266). In addition, all deskphones support IEEE 802.3af-standard LAN-based power. Before you install a deskphone, verify with the LAN administrator whether the LAN supports IEEE 802.3af, and if so, whether the deskphone should be powered locally or by means of the LAN.

When you add devices like multiple button modules or a USB device to applicable IP deskphones, the power class might change. Ensure that all the button modules are of the same model type. The table **Impact of Additional Devices on Telephone Power over Ethernet Power Class** on page 21 shows the effect of such additions on the power class and indicates how to set the IEEE power switch on the back of the deskphone to accommodate different power needs. When you add USB devices, the deskphone displays instructions for any additional power needs.

Note:

The 9621G is a PoE Class 2 device with a 10/100/1000 switch and does not have an IEEE power switch. The 9601 and 9621G do not support a button module, a USB device, or a Dual Headset Adapter.

Note:

If you set the IEEE switch on the back of the deskphone to H, the deskphone registers as a Class 3 device, even if the actual power usage is applicable to Class 1 or 2.

Table 1: 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

Table continues…

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)
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:

The deskphone monitors power consumption to conform to the IEEE 802.3af specifications. If you connect a Dual Headset Adapter (DHA), the power classification might change and you must then change the switch setting as well.

Important:

The last step in assembling the 9600 Series IP Deskphone is to plug in the deskphone with any modules or adapters or both but without attachments such as USB devices and headsets. Plug in the deskphone to a power source either by plugging the power cord into the power source (local power) or plug the modular line cord into the Ethernet wall jack (IEEE power).

Caution:

Failure to connect the proper cables with the proper jacks might result in an outage in part of your network.

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

Deskphone Model:	See figure:
9608, 9608G, 9611G	Connection jacks on a 9608, 9608G, or 9611G deskphone **Note:** The 9601 deskphone has an external power adapter. Use the connections that apply.
9621G, 9641G, 9641GS	Connection jacks on a 9621G, 9641G, or 9641GS deskphone

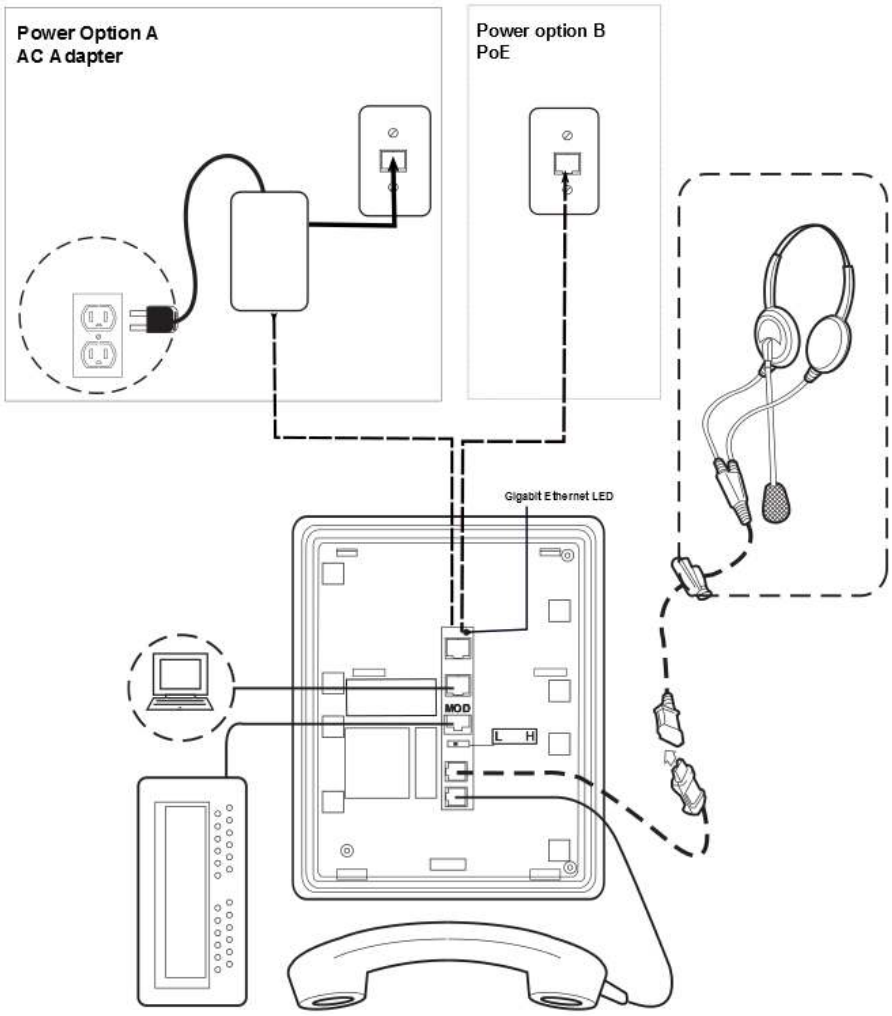
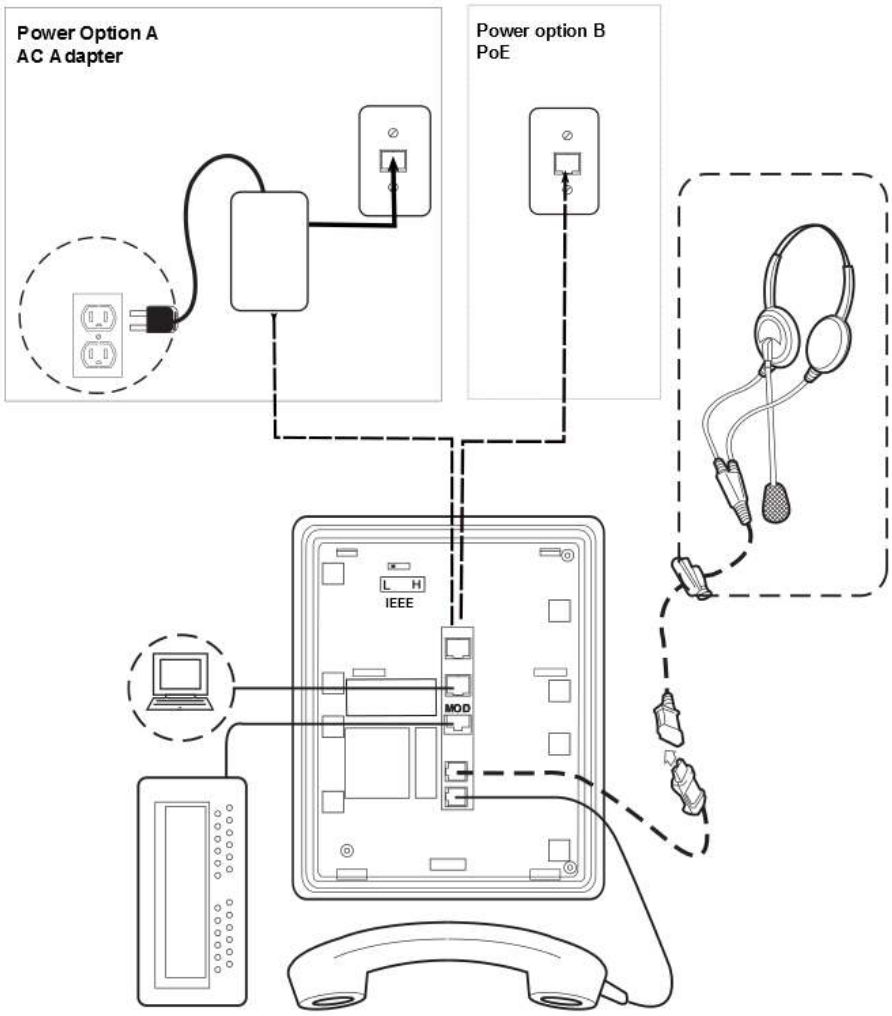


Figure 1: Connection jacks on a 9608, 9608G, or 9611G deskphone

Note:

The Gigabit Ethernet LED indicator is applicable to the 9608G and 9641GS IP deskphones. 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



Note:

The 9621G does not support a button module, USB device, or a Dual Headset Adapter.

Signaling protocol administration

The deskphones are shipped with the H.323 protocol as default. You must convert the signaling to SIP to use the deskphone in a SIP environment. Set the SIG parameter to SIP by using one of the following methods:

- In DHCP Option 242 (Site-Specific Option Number) or in the 46xxsettings.txt file, set the SIG parameter to SIP.
- In the Craft procedure, set the SIG option to SIP.

Post-installation checklist

To ensure that the deskphone is properly installed, verify that the following requirements are complete.

Requirement	Reference	Status
Has the deskphone acquired an IP address?		
Are able to make a call from the deskphone?	See *Using Avaya 9608/9608G/9611G IP Deskphones SIP*, *Using Avaya 9621G/9641G/ 9641GS IP Deskphones SIP*.	
Are you able to perform backup-restore?		
Are you able to change deskphone settings?	See Accessing Craft procedures during normal operation on page 31.	
Are you able to upgrade your phone?		
For security considerations, have you configured the deskphone setup with TLS signaling? Have you installed the appropriate private network authentication certificates?	See *Administering Avaya 9601/9608/9608G/ 9611G/9621G/9641G/ 9641GS IP Deskphones SIP*.	

Chapter 4: Security configurations

Certificate management

The applications running in the 9600 Series IP Deskphones setup rely on trusted certificates for secure operation. The trusted certificate repository can be configured through a parameter, which is used by various applications in the following manner:

- SIP/TLS: Uses the trusted certificates if the certificates are configured, else uses the default Avaya SIP Product CA and Avaya Product Root CA certificate.
- PPM/HTTPS/TLS: Uses the trusted certificates if the certificates are configured, else uses the default Avaya SIP Product CA and Avaya Product Root CA certificate.
- Software distribution package and settings file downloaded from the HTTPS server: Uses the trusted certificates if the certificates are configured, else uses the Avaya Product Root CA certificate. The identity certificate generated using SCEP is used if the deskphone identity certificate is requested by the file server for mutual authentication.
- Ethernet 802.1x EAP-TLS: Uses the trusted certificates. The identity certificate generated using SCEP is used as it is required for authentication.

Enterprises can set up their own certificate authority (CA) by replacing the default Avaya root certificates and Avaya Product Root CA certificates with their trusted certificates. The certificates issued by CA must be configured in the settings file when the 9600 Series IP Deskphones is registered with the enterprise. In addition to root certificates, high-security enterprises install a unique identity certificate on each 9600 Series IP Deskphones. Identity certificates are required if the communication setup is using EAP-TLS, or any other server that requires mutual authentication.

The 9600 Series IP Deskphones support the Simple Certificate Enrollment Protocol (SCEP) to retrieve and load the identity certificates. You can configure SCEP settings in the settings file. If the device is preconfigured, you must return to factory defaults before performing the security configurations.

Note:

The deskphone can only use certificates in PEM format. The MIME type associated with the file-extension of the certificate file that is returned by the HTTP server must be plain/text.

Parameter configuration for secure installation

For secure installation, configure the following parameters.

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

SCEP parameters

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

Parameter	Type	Default value	Description
MYCERTURL	String	Null	Specifies the URL to access Simple Certificate Enrollment Protocol (SCEP) server. The device attempts to contact the server only if this parameter is set to other than its default value.
MYCERTCN	String	$SERIALNO	Specifies the Common name (CN) for SUBJECT in SCEP certificate request. The values can either be $SERIALNO or $MACADDR. If the value includes the string $SERIALNO, that string will be replaced by the phones serial number. If the value includes the string $MACADDR, that string will be replaced by the phones MAC address.
MYCERTDN	String	Null	Specifies common part of SUBJECT in SCEP certificate request. This value defines the part of SUBJECT in a certificate request including Organizational Unit, Organization, Location, State, and Country that is common for requests from different devices.
MYCERTKEYLEN	Numeric	2048	Specifies the private key length in bits to be created in the device for a certificate enrollment. The range is from 1024 to 2048.
MYCERTRENEW	Numeric	90	Specifies the percentage used to calculate the renewal time interval out of the device certificate's Validity Object. If the renewal time interval has elapsed the phone starts to periodically contact the SCEP server again to renew the certificate. The range is from 1 to 99.

Table continues…

Parameter	Type	Default value	Description
MYCERTWAIT	Numeric	1	Specifies the behavior of the device when performing certificate enrolment. assign one of the following values: • 0: Periodical check in the background • 1: Wait until a certificate or a denial is received or a pending notification is received
MYCERTCAID	String	CAIdentifier	Specifies the Certificate Authority Identifier. Certificate Authority servers may require a specific CA Identifier string in order to accept GetCA requests. If the device works with such a Certificate Authority, the CA identifier string can be set through this parameter.
SCEPPASSWORD	String	$SERIALNO	Specifies a challenge password to use with SCEP. The value of SCEPPASSWORD, if non-null, is included in a challengePassword attribute in SCEP certificate signing requests. If the value contains $SERIALNO, $SERIALNO is replaced by the value of SERIALNO. If the value contains $MACADDR, $MACADDR is replaced by the value of MACADDR without the colon separators.

VLAN

Configure the following VLAN parameters.

Parameter	Set to	Notes
VLANSEP	1	Enables the VLAN separation.
L2Q	0, 1, or 2	Specifies 802.1Q tagging mode.
PHY2VLAN	Non-zero value	This is the data VLAN and must not have the same value as the L2QVLAN parameter.
L2QVLAN	Non-zero value	This is the voice VLAN and 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.

Chapter 5: Initial administration

Administration through the settings file

You can perform the initial administration, such as setting the language and time format, through the settings file. Assign appropriate values to the following parameters in the settings file. You can also configure additional parameters as required. For more information and a complete list of the settings file parameters, see *Administering Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP*.

.

- ISO_SYSTEM_LANGUAGE: Sets the language.
- TIMEFORMAT: Sets the time format.
- GMTOFFSET: Specifies the offset from the Greenwich Mean Time.
- DECTSTAT: Specifies whether the DECT menu option in the Settings app is displayed to the user.
- COUNTRY: Specifies the country of operation for specific dial tone generation, Wi-Fi, DECT, and the default anti flickering frequency for camera – 50 Hz or 60 Hz.

Administration through the deskphone

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 deskphone installation for your specific operating environment. This section provides a description of each local administrative option covered in this guide.

Note:

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

Options	Purpose
802.1X	Specifies the 802.1X operational mode.
ADDR	Specifies the network address information.
AGC	Enables or disables Automatic Gain Control.
CALIBRATION	Calibrates the touchscreen (9621G and 9641G models only).
CLEAR	Clears all values to factory defaults.
DEBUG	Enables or disables Debug Mode.
GROUP	Sets the Group Identifier.
HANDSET EQ	Sets the handset equalization.
INT	Specifies the network interface control.
LOG	Enables or disables the event logging.
LOGOUT	Logs off the deskphone.
RESET VALUES	Resets system initialization values to default.
RESTART PHONE	Restarts the deskphone.
SIG	Sets the signaling protocol download flag.
SIP	Configures the SIP call settings.
SNTP	Configures the time server settings.
SSON	Sets the Site-Specific Option Number.
VIEW	Shows current parameter values and file names.

Accessing the local or the Craft procedures

The Local or the Craft procedures can only be invoked if the value of the PROCSTAT parameter in the settings file is set to **0**. Setting the PROCSTAT parameter to **0** provides full access to the local procedures. You can access the Craft menu during deskphone startup and during normal deskphone operation.

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.

Note:

The phone restarts after exiting the craft menu.

Related links

Accessing Craft during deskphone startup on page 31
Accessing Craft procedure during normal operation on page 31

Accessing Craft during deskphone startup

About this task

You can access the Craft menu during deskphone startup using the following steps.

Before you begin

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

Procedure

1. Press **Program** to display the Craft screen.
2. Enter the local dialpad procedure password (0 to 7 numeric digits).
3. Press the **Enter** softkey.

Related links

Accessing the local or the Craft procedures on page 31

Accessing Craft procedure during normal operation

Procedure

1. To run the local procedures, press the **Mute** button, enter the Craft password, and press the pound (#) key.

   A six second time-out is in effect between button presses after you press the **Mute** button. If you do not press a valid button within 6 seconds of pressing the previous button, the phone discards the collected digits. In this case, no administrative option is run.

2. For non-touch screen phones, use the navigation arrows to scroll to and highlight the local procedure you want, then press **Select** or **OK**.

   You can also scroll to the procedure you want, then press the corresponding line button. For touch screen phones, tap the option on the screen.

Related links

Accessing the local or the Craft procedures on page 31

Setting the 802.1x operational mode

About this task

Use the following procedure to set or change the operational mode.

Before you begin

The DOT1X configuration parameter must be set to "0" or "1" for the deskphone to support 802.1X pass-thru and the DOT1XSTAT configuration parameter must be set to "1" or "2" for the deskphone to support supplicant operation.

Procedure

1. Enter the local procedure (Craft) screen using the password as explained earlier.
2. Select **802.1X** option from the screen.

   The following parameters are listed:

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

   two settings shown 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 or the navigation arrows to cycle through the settings.
   - 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** to store the new setting.

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

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

Assigning static IP address

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

Procedure

1. In the Craft 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.
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 Craft 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***.
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

Table continues…

Configuration Parameter Name	Description
	- "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

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 Craft 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.

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

To calibrate the touch screen, use the following procedure:

Procedure

1. Enter the Craft menu using the password.

2. Select the **CALIBRATE SCREEN** form the screen.
3. Choose one of the following options:
   - **Cancel**: Returns to the Craft menu screen without calibrating.
   - **Default**: Resets the calibration parameters to the factory default.
   - **Start**: Calibrates 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 Clear procedure

The **Clear** option erases all administered data — static programming, file server and call server programming, and user settings, and restores all such data to default values. This option does not affect the software load. If you have upgraded the deskphone, the deskphone retains the latest software. Once you have cleared a deskphone, you can administer it normally.

Caution:

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

About this task

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

Procedure

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **CLEAR** from the Admin Procedures screen, the deskphone displays a confirmation screen.
3. If you do not want to clear all values, press **No** to terminate the procedure and retain the current values. Press **Yes** to clear all values to their initial default values. Following values are cleared:
   - The 802.1X identity and password.
   - All system values and system initialization values.
   - User options, parameter settings, identifiers and password.
   - Any user data like Contact Lists or Call Logs are deleted.

   After clearing the values, the deskphone restarts.

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.
- 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 Admin Procedures screen.
2. Navigate to **DEBUG** from the Admin 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 the Group identifier

About this task

Use the following procedure to set or change the Group Identifier.

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 Admin Procedures screen. The default password is **27238**.
2. Select **GROUP** from the Admin Procedures screen.
3. Enter a valid **Group** value (0-999).

   Any changes that you make to the Group value results in the restart of the deskphone when you exit the Craft menu.
4. Press **Save** to store the new setting.

Administering audio equalization

Administering audio equalization

Administering audio equalization

The Federal Communication Commission (a branch of the US Government) in its Part 68 standard, has made Hearing Aid Compatibility (HAC) a mandatory requirement. 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.

Related links

Setting the handset audio equalization on page 38

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**.

Related links

Administering audio equalization on page 38

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 Admin Procedures screen. The default password is **27238**.
2. When you select **INT...** from the Admin 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 Admin Procedures screen. The default password is **27238**.
2. When you select **LOG** from the Admin 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 Admin 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.

Clearing the deskphone 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. **CLEAR** from the menu.

   The phone displays the message,

   ```
   Are you sure you want to reset the phone to factory defaults? This operation
   cannot be undone.
   ```

2. Tap **Yes** to clear all values to use initial default values.

   Tap **No**. 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.

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 deskphone displays the following text:

   ```
   Are you sure you want to reset the phone's initialization values?
   ```

2. Press **No** to return to the screen without resetting the deskphone.

   Press **Yes** to start the deskphone reset.

   The deskphone resets from the beginning of registration, which might take a few minutes. The deskphone 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.
   - Do not affect user-specified data and settings like Contacts data or the deskphone login and password. To remove this type of data, see Clearing the deskphone settings on page 41.

Restarting the deskphone

About this task

Use the following procedure to restart the deskphone.

Procedure

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is *27238*.
2. When you select **RESTART PHONE** from the Admin Procedures screen, the deskphone displays a confirmation screen with the following message:

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

3. Press **No** to return to the Admin Procedures screen without restarting the deskphone. Press **Yes** to proceed with the registration steps

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

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

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 Admin Procedures screen. The default password is **27238**.
2. When you select **SIG...** from the Admin 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 Admin 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 like identifying the SIP Proxy Server.

Procedure

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **SIP** from the Admin Procedures screen, the deskphone displays two choices - SIP Global Settings or SIP Proxy Server.
3. To change any of the SIP Global Settings, press **Select** or **OK** or the corresponding line button and proceed to the next step. To change the SIP Proxy Server(s), scroll down and press **Select** or **OK** or the corresponding line button and proceed instead to Step 4.

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

4. The deskphone displays the Global Settings screen and prompts you to use the Right and Left navigation arrows or a text entry to change a setting and displays the following settings and their active values:

   - **SIP Domain**: Changes the SIP_DOMAIN parameter.
   - **Avaya Environment**: Specifies whether only an Avaya environment (CM and Session Manager) is in effect. There are two modes: **Auto** and **No** and changes the DISCOVER_AVAYA_ ENVIRONMENT parameter.
   - **Reg Policy**: Specifie sthe registration policy for SIP. There are two modes: **alternate** and **simultaneous** and changes the SIPREGPROXYPOLICY parameter.
   - **Failback Policy**: Specifies the fall back policy. There are two modes: **admin** and **auto** and changes the FAILBACK_POLICY parameter.

- **Cfg Srvr**: Specifies the IP address of Avaya configuration server, only if PPM is not on the same server as the SIP Proxy server. The corresponding parameter is CONFIGURATION_SERVER or CONFIGURATION_SERVER _IN_USE.
- **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.

5. If you selected **SIP Proxy Server** the deskphone displays the message "Select SIP proxy to configure" and displays a list of currently configured servers.
6. To add a new server, press **New** and enter the address of SIP Proxy. Then, enter values for the Transport Type and SIP Port as indicated below under changing a setting in Step 6. To change information for a configured server, select the proxy server for which you want to update the Transport Type and/or the SIP Port and press **Select** or **OK**.
7. The deskphone displays the IP Address or DNS Name of the server that you selected and its current Transport Type and SIP Port values. The deskphone prompts you to use the Right and Left navigation arrows or text entry to add/change a setting and displays the following settings and their active values:
   - **SIP Proxy Server**: Specifies the IP address or DNS for Session Manager deployments. The corresponding parameter is SIP_CONTROLLER_LIST .
   - **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.
8. Press **Save** to store the new setting(s) and returns to the Admin Procedures screen.

   You can only change values that have been added using a Local Administrative (Craft) procedure.

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 Admin Procedures screen. The default password is **27238**.

2. When you select **SNTP...** from the Admin 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 Admin Procedures screen.

Setting Site-Specific Option Number

About this task

Caution:

Do not perform this procedure if you are using static addressing. Perform this procedure only if you are using DHCP and the LAN administrator instructs you to do this. Use the following procedure to set the Site-Specific Option Number (SSON).

Procedure

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. When you select **SSON** from the Admin Procedures screen, the following text displays:

   Setting

   where the ***setting*** is the current system value of DHCP_SSON.
3. To change the setting, press the appropriate softkey(s) and use the dialpad to enter a valid SSON value between 128 and 255.
4. Press **Save** to store the new setting and return to the Admin Procedures screen.

Using the VIEW administrative option

Using the VIEW administrative option

If you are using static addressing and encounter problems, use the following procedure to verify the current values of system parameters and file versions.

About this task

Note:

Unless otherwise prevented using administration, the user can view but not change most of the parameters associated with Craft Local Procedures. For more information about this option, see the applicable user guide(s). If the View Network Information option is not available due to being disabled by administration, use the **ADDR** option to view IP Addresses. The IP Addresses might have been entered incorrectly. Verify whether you were provided with correct IP Addresses.

Procedure

1. Use the Craft password to gain access to the Admin Procedures screen. The default password is **27238**.
2. Select **VIEW** from the Admin Procedures screen. See View field descriptions for more details.
3. Press **Back** at any time to return to the Admin Procedures screen.

Related links

VIEW field description on page 47

VIEW field description

Setting	Description	Associated Configuration Parameter
Model	The model of the deskphone that is set by factory procedures. .	MODEL
Application File	The name of the Signed Application/Library software package.	
Kernel/RFS File	The name of the Kernel/ Root File System software package.	
Inactive kernel/ RFS File	The name of the inactive Kernel/ Root File System software package.	
Backup App File	The name of the backup copy of the Signed Application/Library software package stored in the phone.	
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 deskphone.	MACADDR

Table continues…

Setting	Description	Associated Configuration Parameter
SIP Proxy Server	The SIP proxy server to which the deskphone registered successfully.	SIPPROXYSRVR_IN_ USE
Presence Server	The IP address of the presence server.	
Router	The router used as primary gateway out of list of configured routers.	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 startup procedure.	TLSSRVR
HTTP Server	The IP address of the HTTP server that the deskphone accessed before successfully.	HTTPSRVR_IN_USE
DNS Server	The IP address of the DNS server that the deskphone accessed before successfully.	DNSSRVR_IN_USE
SNTP Server	The SNTP server that the deskphone used before to set or update the date and time.	SNTPSRVR_IN_USE
Protocol	Signaling protocol in effect, such as SIP.	
Phone SN	Deskphone Serial Number	
Exchange Server	The Microsoft Exchange™ server that the deskphone uses currently.	EXCHANGE_ SERVER_IN_USE

Related links

Using the VIEW administrative option on page 46

Chapter 6: Backup and restore

PPM backups

The 9600 Series IP Deskphones supports data backup by saving all non-volatile user parameters on Personal Profile Manager (PPM) . When the user logs in to any registered device, PPM restores all user data on the device.

Parameters backed up on PPM

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

Parameter	Default value	Description
BAKLIGHTOFF	120	Specifies the timer to switch off the backlight of the display.
CLICKS	1	Specifies whether button click sounds are enabled.
CALL_PICKUP_RING_TYPE	1	Specifies the default call pickup ring type.
OUTSIDE_CALL_RING_TYPE	1	Specifies the default outside call ring type.
PRIORITY_CALL_RING_TYPE	1	Specifies the default priority call ring type.
INTERCOM_CALL_RING_TYPE	1	Specifies the default intercom call ring type.
TEAM_BUTTON_RING_TYPE_USER_SELECTION	1	Specifies the default team button ring type that the user selects.
FORWARDED_CALL_RING_TYPE	1	Specifies the default forwarded ring type that the user selects.
BRIDGED_CALL_RING_TYPE	1	Specifies the default bridged call ring type that the user selects.
PERSONALWAV	1	Specifies the user choice of the personal ring used for internal calls.
CALL_PICKUP_INDICATION	3	Specifies the following call pickup indication types: • Audio • Visual

Table continues…

Parameter	Default value	Description
		• None
HEADSET_PROFILE	0	Specifies the headset audio profile that the user selects.
AMPLIFIED_HANDSET	0	Specifies whether the handset amplification is enabled.
AMPLIFIED_HANDSET_NOMINAL_LEVEL_CALL_END	0	Specifies whether to set the volume level in amplified mode to nominal when all calls end.
TIMEFORMAT	0	Specifies whether the time format is the am-pm format or the 24–hour format.
DATE_FORMAT_OPTIONS	1	Specifies the date display format.
CALL_LOG_ACTIVE	1	Specifies whether to activate call logging.
CALL_LOG_BRIDGED	1	Specifies whether to activate call logging for bridged calls.
CONTACT_NAME_DISPLAY	1	Specifies how contact names are displayed.
ENABLE_ONLINE_SEARCH	0	Specifies whether the default search directory is searched in the background whenever a user searches through synchronized contacts.
DEFAULT_CONTACTS_STORE	1	Specifies the account where all user contacts are added by default.
EXCHANGE_USER_ACCOUNT	Null	Specifies the account name for the Microsoft Exchange Server account.
EXCHANGE_USER_PASSWORD	Null	Specifies the user password for the Microsoft Exchange Server account.
ENABLE_PHONE_LOCK	0	Specifies whether to enable the lock screen password.
LOCK_SCREEN_LOCK_AFTER_TIMEOUT	5	Specifies the lock screen inactivity timeout in minutes.
SHOW_CALL_APPEARANCE_NUMBERS	0	Specifies whether for a user the device displays call appearance numbers in the call containers.
SHOW_BRIDGED_APPEARANCE_NUMBERS	0	Specifies whether for a user the device displays bridged appearance numbers in the call containers.
AUDIOPATH	1	Specifies whether the default audio path is speaker or headset.
HEADSETBIDIR	0	Specifies whether bidirectional signaling is supported on the headset interface.
LARGEFONT	0	Specifies whether the user selected large font size.
INITIAL_SCREEN	PHONE	Specifies the initial screen that the device displays when the user logs in.
BLOCK_OUTGOING_VIDEO_ANSWER_MODE	0	Specifies whether video is started blocked or unblocked on an incoming or escalated video call.
OUTGOING_CALL_MODE	1	Specifies the media type to be used for outgoing calls.

Chapter 7: Maintenance

Device upgrade

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

- Automatic: You can configure the device to poll periodically for a newer version of the software in the file server and automatically download the software and upgrade itself.
- Manual: You can upgrade the device without the device waiting for a polling interval by:
  - Using the update option in the Settings app on the device. With the update option, the device immediately downloads and installs the software if an updated version is available.
  - Rebooting the device from the Settings app or from System Manager. With rebooting, the device might upgrade immediately or later based on the upgrade policy configured for the device.

Device upgrade process

The upgrade event is logged under NOTICES level in the Syslog file. During boot up, the 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 `9600 Series IP Deskphones`.
3. In the **Choose Release** field, click the required release number.
4. Click the **Downloads** tab.

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

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

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

Related links

File server configuration on page 15

Manual upgrade

Downloading software upgrades

Note:

For any new software release, ensure that you download the latest software distribution package and read any Product Support Notices (PSNs) associated with the new release. Both are available on the Avaya support website

Review the release notes and any Read Me files associated with a distribution package.

Ensure that the settings file is not cached in your browser. To do this, clear the browser cache before downloading the settings file from the Avaya support Web site, so that you don't get an old version.

Software distribution packages containing the files needed to operate the 9600 Series IP Deskphones are packaged together in either a Zip format or RPM/Tar format distribution package. You can download the package appropriate to your operating environment to your file server from the Avaya support website

SIP software distribution packages contain:

- 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.

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, that contains the option settings that enable, disable, or otherwise customize the settings you might need to tailor the deskphones for your enterprise.

Downloading procedure

About this task

The Avaya-provided upgrade script files and the application files included in the zip files upgrade the deskphones. You should not need to modify t hem. It is essential that all the files be together on the file server. When downloading a new release onto a file server with an existing release already on it, you should:

Procedure

1. Stop the file server.
2. If you want to specify a port the deskphones should use to communicate with the file server, administer the desired port setting in HTTPPORT or TLSPORT, for HTTP or TLS, respectively.
3. Back up all the current file server directories as applicable.
4. Copy your ***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 your ***46xxsettings.txt*** file back into the download directory.
9. Check the Readme file for release-specific information.
10. Modify the ***46xxsettings.txt*** file as desired.
11. Restart the HTTP/HTTPS server.
12. Reset your Avaya IP deskphones.

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 deskphone to continue interpreting the settings file at the next line after a **# *tag*** statement. If no such statement exists, the rest of the settings file is ignored.
- Conditionals, of the form **IF *$parameter_name* SEQ *string* GOTO *tag***. Conditionals cause the **Goto** command to be processed if the value of the parameter named ***parameter_name*** exactly matches ***string***. If no such parameter named ***parameter_name*** exists, the entire conditional is ignored. The only parameters that can be used in a conditional statement are: GROUP, MACADDR, MODEL and MODEL4.
- **SET** commands, of the form **SET *parameter_name value***. Invalid values cause the specified value to be ignored for the associated ***parameter_name*** so the default or previously administered value is retained. All values must be text strings, if the value itself is numeric, you must place the numeric value inside a pair of quotation marks. For example, "192.x.y.z"
- Comments, which are statements with characters "**##**" in the first column.
- GET commands, of the form ***GET filename.*** The deskphone 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 deskphone will continue to interpret the original file.

The Avaya-provided upgrade file includes a line that tells the deskphones to **GET *46xxsettings.txt***. This line cause the deskphone 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 deskphone continues processing the upgrade script file. If the settings file is successfully obtained but does not include any setting changes the deskphone stops using HTTP.

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

During a reboot, if the deskphone 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

Table continues…

Parameter	Retained
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
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

Downloading text language files

Language files contain the language name (as it should be presented to a user for selection), an indication of the preferred character input method, text string replacements for the built-in English text strings, where each replacement string may contain up to 120 characters. Each has a unique index that associates it with the corresponding built-in English string, an indication as to whether

Chinese, Japanese or Korean glyphs should be displayed for the Unicode "Unified Han" character codes, and a Language Identification Tag for the language of the text contained in the file. A downloadable language file may also contain a translation of the language name into any or all of the languages for which a language file is included in the software distribution package. Language files must be stored in the same location as the 46xxsettings.txt file.

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

Note:

Language files for SIP deskphones have a **.xml** filename extension whereas language files for 9608, 9608G, 9611G, 9621G, or 9641G IP deskphones 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 deskphones:

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 deskphones 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 9601 deskphone supports only the SIP signaling.

The GROUP parameter

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

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

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

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

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

Chapter 8: Troubleshooting

SLA Mon™ agent

SLA Mon™ technology is a patented Avaya technology embedded in Avaya products to facilitate advanced diagnostics. The deskphones support SLA Mon™ agent which works with a Avaya Diagnostic Server (ADS). SLA Mon™ server controls the the SLA Mon™ agents to execute advanced diagnostic functions, such as:

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

Note:

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

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

Error conditions

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 deskphone 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 9600 Series IP Deskphones 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 deskphone to be IEEE-powered, verify with the LAN administrator that IEEE power is indeed supported on the LAN.

Related links

DTMF tones on page 60
Power interruption on page 60

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 59

Power interruption

If power to 9600 Series IP Deskphone is interrupted while the deskphone is saving the application file, the HTTP/HTTPS application can stop responding. If this occurs, restart the phone.

Related links

Error conditions on page 59

Installation error and status messages

The 9600 Series IP Deskphones issue messages in the currently selected language, or if the deskphone is logged off, in the language specified by the SYSTEM_LANGUAGE parameter value. If English is not the selected language, the deskphone 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 deskphone resets. The most common exception is

`Extension in Use`

, which requires manual intervention.

Possible error and status messages during installation of 9600 Series IP Deskphones

Message	Cause/Resolution
`Address Conflict`	Cause: The deskphone has detected an IP Address conflict. Resolution: Verify administration to identify duplicate IP Address(es).
`Bad Router`	Cause: The deskphone 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 deskphone is proceeding through boot-up. Resolution: Allow the deskphone to continue.
`No Ethernet`	Cause: When first plugged in (or during operation), the SIP IP deskphone 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 deskphone is in the initial stage of rebooting. Resolution: Allow the deskphone 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 deskphone is not on the same VLAN subnet as the router. Resolution: Administer an IP Address on the deskphone using static address or or administer network equipment to administer the deskphone appropriately.
`Updating: DO NOT UNPLUG THE TELEPHONE`	Cause: The deskphone is updating its software image. Resolution: Allow the deskphone to continue.

Operational errors and status messages

The tables described identifies some of the possible operational problems that might be encountered after successful installation of 9600 Series IP Deskphones. The user guide for a specific deskphone model also contains troubleshooting for users having problems with specific deskphone applications.

Possible operational error conditions for 9600 Series IP Deskphones

Condition	Cause/Resolution	
During Craft procedure access, display freezes at prompt "Press * to program"	Cause: Craft access has failed; deskphone cannot operate. Resolution: Unplug the deskphone, then plug it in again to reset.	
After Login, the progress bar shows just a few completed bars and stops moving.	Cause: Login has failed. Resolution: Check that the LAN and File servers are operating correctly. Re-attempt login.	
The message light on the deskphone turns on and off intermittently, but the deskphone never registers.	Cause: This is a hardware fault. Resolution: The deskphone must be returned to Avaya for repair.	
The deskphone stops working in the middle of a call.	No lights are lit on the deskphone and the display is not lit.	Cause: Loss of power. Resolution: Check the connections between the deskphone, the power supply, and the power jack.
	Deskphone might have gone through the restarting sequence.	Cause: Loss of path to the call server or the other party's deskphone, DHCP Lease expired, or DHCP server not available when deskphone attempts to renegotiate DHCP lease. Resolution: Check the connections between the deskphone, the power supply, and the power jack.
The deskphone was working, but does not work now.	No lights are lit on the deskphone and the display is not lit.	Cause: Loss of power. Resolution: Check the connections between the deskphone, the power supply, and the power jack.
	Power to the deskphone 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 deskphone using ARP or trace-route and from the deskphone to the call server by invoking a

Table continues…

		Feature button. Verify that administration has not changed for the LAN equipment (routers, servers, etc.) between the call server and the deskphone. Verify no one changed the deskphone settings locally using the **View** and **ADDR** craft procedures, as described earlier in this guide.
	The deskphone was recently moved.	Cause: Loss of communication with the call server. Resolution: As above, but pay particular attention to the possibility that the deskphone 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 deskphone.
	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 deskphone works, but the audio quality is poor.	The user hears echo when speaking on a handset.	Cause: Echo from digital-to-analog conversion on your Communication Manager call server trunk. Resolution 1: Try a different Call Quality setting under the Audio Parameters section. Resolution 2: Check whether packet loss, or jitter delay is causing this problem, by eliminating or minimizing both. Resolution 3: Verify which trunk is causing the echo, and check the trunk's Trunk Termination parameter on the call server.
	The user hears echo on a headset, but not on a handset.	Cause: Improper headset adapter. Resolution: Replace adapter with Avaya's M12LU or 3412-HIC adapters. We recommend the M12LU, since it supports Automatic Gain Control.

Table continues…

	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 deskphone. 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 deskphone. 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 deskphone 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 deskphone works properly, except incoming DTMF tones are not received.	Cause: The TN2302AP board does not pass in-band DTMF tones. Resolution: None; the board is operating as designed.	
When a line is selected, a short dial tone burst sounds followed by a reorder/fast busy tone.	Cause: The extension is provisioned on Session Manager and some Communication Manager forms, but not on the off-pbx-telephone station-mapping form. Communication Manager is unable to map back to Session Manager, and rejects the line reservation. Resolution: Map the extension on the off-pbx-telephone station-mapping form. Cause: Possible error in SIG group configuration on Communication Manager, which indicates the default region for the SIP trunk to Communication Manager.	

Table continues…

	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 deskphone).	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 deskphone.	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 deskphone administration recently changed.	Cause: The ***96xxSupgrade.txt*** file was edited incorrectly, renamed, etc. Resolution: Download a clean copy of the ***96xxSupgrade.txt*** file from the Avaya support siteand do not edit or rename it. Customize or change only the ***46xxsettings*** file.
The MS Exchange contacts take too long to load	Cause: The correct Exchange server is not specified in the parameter EXCHANGE_SERVER_LIST in the ***46xxsettings*** file. Resolution: Verify that the MS Exchange server being used is specified in the settings file. To view the Exchange server in use, go to: **Outlook** > **Tools>Options** > **Mail Setup** > **E-mail Accounts** > **Change** .	
Some settings in the settings file are being ignored while other settings are being used properly.	Cause: Improper settings file administration. Resolution: Verify that customized settings are correctly spelled and formatted.	
	The setting being ignored is one or more of the AGC settings.	Cause: The user changed the AGC setting(s). Resolution: Have the user reset the AGC value(s) back to the desired setting(s).
	The setting being ignored is the TIMEFORMAT setting.	Cause: The time format was changed using the Avaya Menu Options & Settings. Resolution: If the time disappears, Reboot the phone.
Deskphone power is interrupted while the deskphone is saving the	Cause: The HTTP/HTTPS application stops responding if power is interrupted while a deskphone is saving the application file.	

Table continues…

application file and the HTTP/ HTTPS application stops responding.	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 deskphone and logged into another deskphone.	Cause: Possible PPM problem. Resolution: Contact the Session Manager administrator.
The deskphone 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".
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 9601, 9608, 9608G, 9611G, 9621G, 9641G, or 9641GS IP deskphone also assumes

that no encryption is an option provisioned in Communication Manager. If Communication Manager is provisioned with the cryptosuite aescm128-hmac80, then the following entry must be in the 46xxsettings.txt file:

SET MEDIAENCRYPTION "1,9"

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

Chapter 9: Related 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.	For 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.	For people who want to gain a high-level understanding of the Avaya Aura® Session Manager features, functions, capacities, and limitations.
Implementing		
Deploying Avaya Aura® Session Manager	See the installation procedures and initial administration information for Avaya Aura® Session Manager.	For people who install, configure, and verify Avaya Aura® Session Manager on Avaya Aura® System Platform.
Upgrading Avaya Aura® Session Manager	See upgrading checklists and procedures.	For people who perform upgrades of Avaya Aura® Session Manager.
Deploying Avaya Aura® System Manager on System Platform	See the installation procedures and initial administration information for Avaya Aura® System Manager.	For people who install, configure, and verify Avaya Aura® System Manager on Avaya Aura® System

Table continues…

Title	Use this document to:	Audience
		Platform at a customer site.
Administering		
Administering Avaya 9601/9608/9608G/9611G/9621G/ 9641G/9641GS IP Deskphones SIP	See information about how to perform 9600 Series IP Deskphones administration tasks including how to use management tools, how to manage data and security, an how to perform periodic maintenance tasks.	For people who perform 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 how to perform Avaya Aura® Session Manager administration tasks including how to use management tools, how to manage data and security, an how to perform periodic maintenance tasks.	For people who perform Avaya Aura® Session Manager system administration tasks.
Administering Avaya Aura® System Manager for Release 7.0.1	See information about how to perform Avaya Aura® System Manager administration tasks including how to use management tools, how to manage data and security, an how to perform periodic maintenance tasks.	For people who perform Avaya Aura® System Manager administration tasks.
Maintaining		
Maintaining Avaya Aura® Session Manager	See information about the maintenance tasks for Avaya Aura® Session Manager.	For people who maintain Avaya Aura® Session Manager.
Troubleshooting Avaya Aura® Session Manager	See information for troubleshooting Avaya Aura® Session Manager, resolving alarms, replacing hardware, and alarm codes and event ID descriptions.	For people who troubleshoot Avaya Aura® Session Manager.

Related links

Finding documents on the Avaya Support website on page 69

Finding documents on the Avaya Support website

About this task

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

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.

4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

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

Related links

Documentation on page 68

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

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

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

O

P

R

S

T

U

V