



Installing and Administering Avaya 9600 Series and J100 Series IP Phones H.323

Release 6.8.5
Issue 1
November 2020

Note

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL

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

Australia Statements

Handset Magnets Statement:

**Danger:**

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

Industry Canada (IC) Statements**RSS Standards Statement**

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

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

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

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

Radio Transmitter Statement

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

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

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

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

Radiation Exposure Statement

This equipment complies with FCC & IC RSS102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Cet équipement est conforme aux limites d'exposition aux rayonnements ISEDétablies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

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

Japan Statements**Class B Statement**

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

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

取扱説明書に従って正しい取り扱いをして下さい。 VCCI-B

Denan Power Cord Statement**Danger:**

Please be careful of the following while installing the equipment:

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

**警告**

本製品を安全にご使用頂くため、以下のことにご注意ください。

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

México Statement

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

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

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

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

Brazil Statement

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

Power over Ethernet (PoE) Statement

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

Taiwan Low Power Radio Waves Radiated Devices Statement

802.11b/802.11g/BT:

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

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

低功率電波輻射性電機管理辦法

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

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使

用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

U.S. Federal Communications Commission (FCC) Statements

Compliance Statement

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

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

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

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

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

Class B Part 15 Statement

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

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

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

Radiation Exposure Statement

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

ENERGY STAR® compliance statement



As an ENERGY STAR partner, Avaya Inc. has determined that this product meets the ENERGY STAR guidelines for energy efficiency. Information on the ENERGY STAR program can be found at www.energystar.gov. ENERGY STAR and the ENERGY STAR mark are registered trademarks owned by the U.S. Environmental Protection Agency.

EU Countries

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

Avaya J159 IP Phone, Avaya J179 IP Phone, and Avaya J189 IP Phone complies with the EMC Directives.

WiFi transmitter

For Avaya J159 IP Phone, Avaya J179 IP Phone, and Avaya J189 IP Phone

- Frequencies for 2412-2472 MHz, transmit power: < 20 dBm
- Frequencies for 5180-5240 MHz, transmit power: < 20 dBm

BT transmitter

For Avaya J179 IP Phone and Avaya J189 IP Phone:

- Frequencies for 2402-2480 MHz, transmit power: < 6.0 dBm

General Safety Warning

- Use only the Avaya approved Limited Power Source power supplies specified for this product.
- Ensure that you:
 - Do not operate the device near water.
 - Do not use the device during a lightning storm.
 - Do not report a gas leak while in the vicinity of the leak.
 - For Accessory Power Supply in Avaya J100 Series IP Phones— Use Only Limited Power Supply Phihong Technology Co. Ltd. Model: PSAC12R-050, Output: 5VDC, 2.4A.

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.

The Bluetooth™ word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Avaya Inc. is under license.

Device Usage Consent

By using the Avaya device you agree that Avaya, from time to time, may collect network and device data from your device and may use such data in order to validate your eligibility to use the device.

Contents

Chapter 1: Introduction	11
Purpose	11
Change history	11
Chapter 2: Avaya 9600 and J100 IP Phones overview	13
Phone overview	13
Avaya 9600 IP Deskphone Models	14
Avaya J100 IP Phone Models	15
Hardware dimensions and specifications for Avaya 9600 Series phones	16
Hardware dimensions and specifications for Avaya J100 Series phones	18
Power specification for 9600 Series Phone	20
Power specifications for J100 Series IP Phones	22
Optional components for J100 IP Phone	23
Secondary display	23
Button modules	23
Chapter 3: Initial setup and connectivity	25
Installing the 9600 and J100 IP phones	25
Prerequisites	26
Diagram: IP phone setup	30
Upgrading the phones	31
Updating phone software for installation	31
Plugging in the IP phones	32
Completing the power connection for 9600 Series Deskphones	37
Installing a Dual Headset Adapter (DHA)	37
Installing 9641G Call Center faceplate	42
Plugging in and resetting the phones using the Dynamic Addressing Process	43
Understanding the plug in and reset process	43
Understanding Unnamed registration	47
Wall mounting Avaya J100 Series IP Phones	48
Wall mounting Avaya J100 Expansion Module	50
Local Administration menu procedures	52
Running Craft procedures	53
Accessing the Administration menu after phone startup	54
Entering data for administrative options	54
Entering and validating IPv4 and IPv6 addresses	55
Local administrative Craft procedures menu	57
Setting the operational mode to 802.1X	58
Changing IP address information	59
Clearing the phone settings	61
Debug mode	62

Changing Ethernet interface control.....	63
Disabling and enabling event logging.....	64
Logging off from the phone.....	65
Viewing multilanguage strings.....	66
Resetting system values.....	66
Restarting the phone.....	67
Setting or changing the signaling protocol.....	67
Changing SSON settings.....	68
Performing a self-test.....	69
Post installation checklist for 9600 and J100 IP Phones.....	70
Chapter 4: Administering your phone.....	71
Administrator responsibilities.....	71
Logging in to your phone as an administrator.....	71
Initial administration checklist.....	72
Administrative requirements.....	73
Parameter data precedence.....	74
Initialization process overview.....	74
JITC security compliance mode overview.....	79
Error conditions.....	85
Network requirements.....	85
Network assesment.....	85
Hardware requirements.....	86
Server requirements.....	86
Required network information.....	87
Other network considerations.....	87
Communication Manager Administration.....	98
Call server requirements.....	98
Call server administration.....	99
Administering Voice mail.....	101
Call transfer administration.....	102
Call conferencing.....	102
Administering deskphones on Avaya Aura® Communication Manager	104
Station administration.....	106
Aliasing phones for switch compatibility.....	107
Administering feature and call appearance labels.....	107
Server Administration.....	107
Software prerequisites.....	107
Administering the DHCP and file servers.....	108
DHCP generic setup.....	109
Setting up the DHCP server.....	109
Setting up a DHCPv6 server.....	116
HTTP generic setup.....	116
Backup and restore processing.....	118

About IPv4 and IPv6 operation.....	120
Features not supporting IPv6.....	121
Telephone Software and Application Files.....	122
Understanding the general download process.....	122
Using the GROUP parameter to set up customized groups.....	125
Administering Deskphone Options.....	126
Administering options.....	126
H.323 customizable system parameters.....	127
Single Sign on for local devices (SSON-LD).....	165
Administering a VLAN.....	166
About DNS addressing.....	168
EAP-TLS support for authentication.....	168
About IEEE 802.1X.....	173
About Link Layer Discovery Protocol (LLDP).....	175
Administering settings at the phone.....	179
Administering display language options.....	180
Administering dialing methods.....	182
About internal audio parameters.....	182
Managing applications on the Home screen.....	183
Administering features on softkeys.....	185
Administering a custom screen saver.....	192
About administering audio equalization.....	193
About Acoustic protection.....	194
Configuring phone based auto-answer.....	195
Administering backup and restore.....	197
Administering Applications and Options.....	202
Customizing Applications and Options.....	203
Setting the Application Status flag.....	203
Administering the Avaya menu.....	205
Sample Avaya Menu Administration File Template.....	205
Administering guest users.....	208
Administering visiting users	208
Idle timer configuration.....	208
Chapter 5: Administration overview and requirements.....	210
Parameter data precedence.....	210
Initialization process overview.....	210
Connection to network.....	211
DHCP processing.....	211
File downloads.....	211
Certificates usage.....	212
Registration with the call server.....	213
JITC security compliance mode overview.....	215
JITC security compliance mode configuration.....	216

Error conditions.....	221
Chapter 6: Maintaining an Avaya IP Phone.....	222
Upgrading the device.....	222
Downloading and saving the software.....	222
Upgrading the device manually.....	223
Downloading text language files.....	224
Avaya J100 Expansion Module upgrade.....	224
Software distribution packages.....	225
Upgrading software packages.....	226
Contents of the settings file.....	227
Settings file parameters retained during reboot.....	228
Downloading text language files.....	231
Changing the signaling protocol.....	231
Applying settings to logical groups.....	232
Calibrating the touch screen.....	232
Adjusting contrast on the button module.....	233
Adjusting contrast on button modules and non-color deskphones.....	234
Disabling or enabling automatic gain control.....	234
Setting handset audio equalization.....	235
Changing the group identifier.....	236
Chapter 7: Data Privacy for 9600 and J100 IP Phones H.323.....	237
Data Privacy detailed description.....	237
Data Privacy Controls.....	237
User information storage or sending over the network	237
Encryption of user information.....	238
Access to user data.....	238
Data retention.....	239
Management of user data.....	239
Recommendation for better securing user information.....	240
Data privacy controls for Avaya J100 Series H.323 and 9600 IP Phones.....	241
Chapter 8: Troubleshooting.....	247
Resolving error conditions.....	247
Failure to hear DTMF tones.....	247
Correcting a power interruption.....	248
Using the VIEW procedure for troubleshooting.....	248
Installation error and status messages.....	251
Operational errors and status messages.....	255
LLDP Troubleshooting.....	260
Proposed Solution.....	261
LLDP setup and troubleshooting steps.....	261
Proposed solution for DHCP configured deskphones.....	262
Proposed solution for script-configured deskphones.....	262
Proposed solution for LLDP-configured deskphones.....	262

SLA Mon™ agent..... 263

Secure Shell Support..... 263

Troubleshooting Avaya J100 Expansion Module..... 264

 Debugging the expansion module..... 265

Chapter 1: Introduction

Purpose

This document contains information about installing, deploying, administrating, maintaining, and troubleshooting of 9600 Series IP Deskphones and Avaya J100 Series IP Phones.

This document is intended for the deployment engineers or support personnel who install, administer, and maintain 9600 Series IP Deskphones and Avaya J100 Series IP Phones.

Knowledge

- DHCP
- H.323
- Installing and configuring Avaya Aura[®] components
- Installing and configuring IP Office components
- 802.1x and VLAN

Skills

Administering and configuring:

- Avaya Aura[®] Communication Manager
- Avaya Aura[®] Presence Services
- IP Office
- DHCP server
- HTTP or HTTPS server

Tools

- Avaya Aura[®] System Manager
- IP Office Manager
- IP Office Web Manager

Change history

Issue	Date	Summary of changes
Release 6.8.3	12–Nov-2019	Merged documentation for installing and administering procedures. Updated for H.323 6.8.3 release.
Release 6.8.5	24–Nov-2020	Added contents for J189 and J159 device. Updated for H.323 6.8.5 release.

Chapter 2: Avaya 9600 and J100 IP Phones overview

Phone overview

9600 Series IP Deskphones and Avaya J100 Series IP Phones are phones for business communications. Avaya 9600 and J100 Series IP phones are a set 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. It works with the Avaya Aura[®] environment to provide a flexible architecture that works with your investments and accommodates growth as your business needs change. These IP phones offer high audio quality and low power requirements and the flexibility to customize. With the high-performance models of series that can operate in H.323 you can use the phones to:

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

9600 Series IP Deskphones and Avaya J100 Series IP Phones phones have an integrated Ethernet port. You can connect your computer to the Ethernet through your phone, so that one Ethernet port can be utilized for both the devices.

Types of H.323 protocols used in 9600 Series IP Phones

The H.323 standard provides real time audio, video, and data communications transmission over a packet network. An H.323 telephone protocol stack comprises several protocols:

- H.225 for registration, admission, status (RAS), and call signaling
- H.245 for control signaling
- Real Time Transfer Protocol (RTP) and Secure Real Time Transfer Protocol (SRTP)

- Real Time Control Protocol (RTCP) and Secure Real Time Control Protocol (SRTCP)



Caution:

Ensure that adequate technical support is available for servers used with any 9600 Series IP Deskphones system.

This document does not describe how to use the 9600 Series IP Deskphones and J100 Series IP Deskphones in an IP Office environment.

Enhancements in 9600 Series IP Deskphones

General enhancements:

- Supports user settings for volume on reboot and login.

Security enhancements:

- Supports the use of TLS in conjunction with TTS (Time To Service).
- Supports H.323 signaling over TLS.
- Supports EAP-TLS 1.2.
- Supports SHA-2 signature image.
- Supports TLS_VERSION and CTASTAT

Administrative features:

- Recovery from incorrect credentials using the Reset softkey when the deskphone is in the discovery and registering mode.

Avaya 9600 IP Deskphone Models

Table 1: Available 9600 IP deskphone models

Deskphone model	Features
9608	You can use up to eight lines and administer graphical labels centrally for the deskphone. The deskphone supports a traditional user interface and a graphical monochrome display. The deskphone includes graphical labels that you can administer centrally and thereby avoid use of paper labels.
9608G	You can use up to eight lines and administer graphical labels centrally for the deskphone. The deskphone supports a traditional user interface and a graphical monochrome display. The deskphone includes graphical labels that you can administer centrally and thereby avoid use of paper labels. 9608G deskphone supports Gigabit Ethernet connectivity.

Table continues...

Deskphone model	Features
9611G	The 9611G has a traditional user interface and a graphical color display. The deskphone includes graphical labels that you can administer centrally. You can use up to eight lines with the 9611 deskphone. The 9611 deskphone supports integrated Gigabit and a USB interface. The deskphone has a 3.5 inch graphical color display with a white backlight.
9621G	The 9621G IP deskphone delivers gigabit capability and touch screen functionality on a 4.3 inch color touch screen. Customers with a need for gigabit connectivity to the desktop prefer the 9621G deskphone.
9641G	The 9641G deskphone delivers advanced capabilities with 4.7 inch wide color touch screen, wideband speaker, USB interface, Bluetooth 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 9641 deskphone.
9641GS	The 9641GS deskphone has a 5.0 inch TFT capacitive touch screen that provides better touch sensitivity. This deskphone supports the Ethernet link and activity LED for the network port, in addition to providing USB interface, Bluetooth 3.0, and gigabit capability.

Avaya J100 IP Phone Models

The following table lists the available models for Avaya J100 Series IP Phones with their brief description.

Table 2: Available J100 IP phone models

Phone model	Description
J159 IP Phone	<p>J159 phone has two color display with Primary display supporting four call appearances in half-width mode. The Primary display is scrollable that supports up to 96 lines/features/applications.</p> <p>The secondary color display has 6 lines/features/applications buttons and is pagable supporting up to 24 lines/features/applications.</p> <p>The phone does not support button module.</p>
J169 IP Phone	<p>J169 phone has a grayscale display that supports eight call appearances with four lines of call display.</p> <p>The phone can also support up to three button modules each supporting 24 application lines.</p>

Table continues...

Phone model	Description
J179 IP Phone	J179 phone has a color display that supports eight call appearances in half-width mode. The phone can also support up to three button modules each supporting 24 application lines.
J189 IP Phone	J189 has a two color display with primary display supporting ten call appearances in half-width mode. The secondary quick dial display which is an integrated expansion module supports 24 application lines. The phone also support upto two expansion modules supporting 24 application lines in each page.

Hardware dimensions and specifications for Avaya 9600 Series phones

9600 Series IP Deskphone dimensions

Deskphone	Height	Width	Depth
9608	230 mm	204 mm	35 mm without stand
9611G	230 mm	204 mm	35 mm without stand
9621G	230 mm	232 mm	35 mm without stand
9641G	230 mm	232 mm	35 mm without stand
9641GS	230 mm	232 mm	35 mm without stand

Hardware specifications for 9600 series IP Deskphone

Avaya 9600 Series IP Deskphone supports following hardware and physical specification:

Parameter	9608	9611G	9621G	9641G	9641GS
Handset Tx frequency	7 Khz	7 Khz	7 Khz	7 Khz	7 Khz
Handset Rx frequency	7 Khz	7 Khz	7 Khz	7 Khz	7 Khz
Handset cord length and amp; type	9-foot 4-conductor coiled	9-foot 4-conductor coiled	9-foot 4-conductor coiled	9-foot 4-conductor coiled	9-foot 4-conductor coiled
Handset weight	141 gms	141 gms	141 gms	141 gms	141 gms

Table continues...

Parameter	9608	9611G	9621G	9641G	9641GS
Permanently labeled feature buttons	Speaker (w/red LED)	Speaker (w/red LED)	Speaker (w/red LED)	Speaker (w/red LED)	Speaker (w/red LED)
	Headset (w/red LED)	Headset (w/red LED)	Headset (w/red LED)	Headset (w/red LED)	Headset (w/red LED)
	Mute (w/red LED)	Mute (w/red LED)	Mute (w/red LED)	Mute (w/red LED)	Mute (w/red LED)
	Volume (up/down)	Volume (up/down)	Volume (up/down)	Volume (up/down)	Volume (up/down)
	Phone	Phone	Phone	Phone	Phone
	History (w/red LED)	History (w/red LED)	History (w/red LED)	History (w/red LED)	History (w/red LED)
	Contacts	Contacts	Contacts	Contacts	Contacts
	“A” Home	“A” Home	“A” Home	“A” Home	“A” Home
	Message	Message	Message (w/red LED)	Message (w/red LED)	Message (w/red LED)
	Navigation: up, down left, right OK	Navigation: up, down left, right OK	Forwarding (w/red LED)	Forwarding (w/red LED)	Forwarding (w/red LED)
Button Specs	Activation force = 100 to 160 grams, Travel distance = 1.1 to 1.3 millimeters, height = approximately 0.5 millimeter above the housing when fully depressed, A snap ratio of 0.35 +/- 0.1 or higher.	Activation force = 100 to 160 grams, Travel distance = 1.1 to 1.3 millimeters, height = approximately 0.5 millimeter above the housing when fully depressed, A snap ratio of 0.35 +/- 0.1 or higher.	Activation force = 100 to 160 grams, Travel distance = 1.1 to 1.3 millimeters, height = approximately 0.5 millimeter above the housing when fully depressed, A snap ratio of 0.35 +/- 0.1 or higher.	Activation force = 100 to 160 grams, Travel distance = 1.1 to 1.3 millimeters, height = approximately 0.5 millimeter above the housing when fully depressed, A snap ratio of 0.35 +/- 0.1 or higher.	Activation force = 100 to 160 grams, Travel distance = 1.1 to 1.3 millimeters, height = approximately 0.5 millimeter above the housing when fully depressed, A snap ratio of 0.35 +/- 0.1 or higher.
Main display	181 x 120 pixel monochrome no grey levels	3.5 inch 320 x 240 pixel TFT 18 bit color	4.3 inch 480 x 272 pixel TFT 24 bit color	4.7 inch 480 x 272 pixel TFT 24 bit color	5.0 inch 480 x 272 pixel TFT 24 bit color
Display Backlight	White	Yes	Yes	Yes	Yes

Table continues...

Parameter	9608	9611G	9621G	9641G	9641GS
Touch Screen	No	No	Resistive (4 wire)	Resistive (4 wire)	Capacitive
CA/Feature Buttons – main display (physical buttons)	8 with red and green LEDs each	8 with red and green LEDs each	No	No	No
Softkeys call control	4	4	No	No	No
Ethernet Signal range	100 meters (328 feet) on category 5e UTP (unshielded twisted pair) cable.	100 meters (328 feet) on category 5e UTP (unshielded twisted pair) cable.	100 meters (328 feet) on category 5e UTP (unshielded twisted pair) cable.	100 meters (328 feet) on category 5e UTP (unshielded twisted pair) cable.	100 meters (328 feet) on category 5e UTP (unshielded twisted pair) cable.
Ethernet activity LED	No	No	No	No	Yes
Bluetooth	No	No	No	Yes	Yes
Handset	Wideband	Wideband	Wideband	Wideband	Wideband
Hands-free	Narrowband	Narrowband	Wideband	Wideband	Wideband
Microphone and amp type	1 omni-directional	1 omni-directional	1 omni-directional	1 omni-directional	1 omni-directional
PCB Chip	11170	11109	11109	11109	11109
Reliability Rate in Technician Usage rate (the number of units used from repair stock per month per 100 units in the installed base)	Less than or equal to 0.1.	Less than or equal to 0.1.	Less than or equal to 0.1.	Less than or equal to 0.1.	Less than or equal to 0.1.

Hardware dimensions and specifications for Avaya J100 Series phones

Hardware specifications for J100 Series IP Phones

Avaya J100 Series IP Phones support the following hardware specifications:

Standard	J159	J169	J179	J189	JBM24	JEM24
Phone dimensions with the stand in high position	185 mm (7.3 in) Wide x 170 mm (6.7 in) Deep x 224.3mm (8.8 in) Tall	187 mm (7.4 in) Wide x 175 mm (6.9 in) Deep x 183 mm (7.2 in) Tall	187 mm (7.4 in) Wide x 175 mm (6.9 in) Deep x 183 mm (7.2 in) Tall	227 mm (8.9 in) Wide x 179 mm (7.0 in) Deep x 199 mm (7.8 in) Tall	88.2 mm (3.4 in) Wide x 175 mm (6.9 in) Deep x 224.3 mm (8.8 in) Tall	115.5 mm (4.5 in) Wide x 175 mm (6.9 in) Deep x 173.64 mm (6.8 in) Tall
Phone dimensions with the wall mount	185 mm (7.3 in) Wide x 98.83 mm (3.9 in) Deep x 225.24 mm (8.9 in) Tall	187 mm (7.4 in) Wide x 100 mm (3.9 in) Deep x 225 mm (8.9 in) Tall	187 mm (7.4 in) Wide x 100 mm (3.9 in) Deep x 225 mm (8.9 in) Tall	227 mm (8.9 in) Wide x 100 mm (3.9 in) Deep x 244 mm (9.6 in) Tall	88.2 mm (3.4 in) Wide x 100 mm (3.9 in) Deep x 224.3 mm (8.8 in) Tall	115.5 mm (4.5 in) Wide x 100 mm (3.9 in) Deep x 173.64 mm (6.8 in) Tall
Wall mountable	Yes	Yes	Yes	Yes	Yes	Yes
Stand	Dual-position	Dual-position	Dual-position	Dual-position	Dual-position	Dual-position
Call appearances	4 on primary display and 24 on secondary display	8	8	10 on primary display and 24 on secondary display.	N/A	N/A
Display type	Color	Grayscale	Color	Color	Grayscale	Grayscale and color
Display	<ul style="list-style-type: none"> Main display: 2.8", 320 x 240 pixels Secondary display: 2.4", 240 x 320 pixels 	3.5", 320 x 240 pixels	3.5", 320 x 240 pixels	Main display: 5", 800 x 480 pixels Secondary display: 2.4", 240 x 320 pixels	3.3", 160 x 320 pixels	4.3", 272 x 480 pixels
Dual color call indicator	4	8	8	10	0	24
Ethernet switch	Dual 10/100/1000	Dual 10/100/1000	Dual 10/100/1000	Dual 10/100/1000	N/A	N/A
Wi-Fi support	No	No	No	No	N/A	N/A
Soft keys call control	4	4	4	4	N/A	two keys to switch between active pages

Table continues...

Standard	J159	J169	J179	J189	JBM24	JEM24
Wired handset	Yes	Yes	Yes	Yes	N/A	N/A
Amplified handset mode	Yes, with 20dB of gain	Yes, with 20dB of gain	Yes, with 20dB of gain	Yes, with 20dB of gain	N/A	N/A
Wired headset	Yes	Yes	Yes	Yes	N/A	N/A
Bluetooth support	No	No	No	No	N/A	N/A
Expansion module capable	No	Yes (3)	Yes (3)	Yes (2)	N/A	N/A
Optional DC power	Yes	Yes	Yes	Yes	N/A	N/A
PoE ¹	Yes	Yes	Yes	Yes	N/A	N/A
USB port	No	No	No	Yes	No	No

Power specification for 9600 Series Phone

Power Specifications for 9600 Series IP deskphones

Avaya 9600 Series H.323 IP deskphones work on the standard Power over Ethernet (PoE) 5 specification of 802.3af. The specification provides for up to 15.4 W of DC power that has a voltage of minimum 44 V DC and a current specification of 350 mA for each device.

Phone model	IEEE power classification	Typical power usage, conservation mode disabled (in W)	Typical power usage, conservation mode enabled, backlight if any turned off (in W)	Maximum power usage (in W)
9608	1	2.08	1.93	2.55
9611G	1	3.12	2.64	3.78
9621G	2	3.49	3.18	4.27
9641G	2	3.44	3.28	4.12

Table continues...

¹ PoE can be supplied from one of the following:

- Direct
- Data switch

Phone model	IEEE power classification	Typical power usage, conservation mode disabled (in W)	Typical power usage, conservation mode enabled, backlight if any turned off (in W)	Maximum power usage (in W)
9641GS	1: When the switch is in the low position. 3: When the switch is in the high position.	2.40	3.55	4.50

Power specifications with button module attachments:

Deskphone	9608/9608G	9611G	9621G	9641G/9641GS
PoE Power support	The 9608 deskphone natively supports Power over Ethernet (802.3af) and has a PoE rating of Class 1 when you do not connect a SMB24 or 12 button x1 module to the deskphone.	The 9611 deskphone natively supports Power over Ethernet (802.3af) and a PoE rating of Class 1 when you do not connect a SMB24 or 12 button x1 module to the deskphone. With the addition of a button module, you can increase the PoE class by one power level i.e. PoE class II. With the addition of three button modules the PoE class does not exceed PoE Class II.	The 9621 deskphone natively supports Power over Ethernet (802.3af) and has a maximum PoE rating of Class II. The deskphone does not support the use of button modules.	The 9641 deskphones natively supports Power over Ethernet (802.3af), and has a maximum PoE rating of Class II when you connect a single button module, either the SBM24 or 12 button x1 module. With the addition of button modules or the USB stick, you can increase the PoE class by one power level i.e. PoE class III.
Power Interface	PoE: IEEE	PoE: IEEE	PoE: IEEE	PoE: IEEE
Power class target	1,2	1,3	2	2,3
Power class switch	Yes	Yes	No	Yes

Power specifications for J100 Series IP Phones

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

Avaya J100 Series IP Phones are ENERGY STAR® compliant.

! Important:

- Avaya J159 IP Phone is a class 1 device and does not support peripherals.
- Avaya J169 IP Phone and Avaya J179 IP Phone supports three JBM24 Button Modules or two Avaya J100 Expansion Modules on PoE. For additional button modules, use 5V DC power adapter.

* Note:

The simultaneous connection of JBM24 Button Module and Avaya J100 Expansion Module is not supported.

- Avaya J189 IP Phone supports two Avaya J100 Expansion Module, with one expansion module supported on PoE. For additional button modules, use 5V DC power adapter.

* Note:

The connection of JBM24 Button Module is not supported by Avaya J189 IP Phone.

- If you are using a power adapter, disable PoE on the Ethernet connection.

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

Phone model	Avaya standard power measurements (in Watts)			Energy Star (in Watts)
	Conservation	Typical	Maximum	Standby
J159	1.75	2.33	3.84	2.04
J169	1.72	1.84	2.34	1.85
J179	1.74	2.10	2.71	1.85
J189	2.32	2.91	3.93	1.92
JBM24	0.19	0.69	1.35	NA
JEM24	1.70	1.90	2.00	NA
USB device (USB Port-A)	NA	NA	2.5	NA

The power requirements of the phone vary depending on the connected peripherals. The following table provides the correlation between the connected peripherals and power requirements.

Phone model	PoE Class
J159	IEEE 802.3af PoE, Class 1 device.

Table continues...

J169	<ul style="list-style-type: none"> • IEEE 802.3af PoE Class 1 without a button module. • IEEE 802.3af PoE Class 2 for one or more button modules.
J179	<ul style="list-style-type: none"> • IEEE 802.3af PoE Class 1 without a button module. • IEEE 802.3af PoE Class 2 for one or more button modules.
J189	<ul style="list-style-type: none"> • IEEE 802.3af PoE Class 2 without a expansion module. • IEEE 802.3af PoE Class 3 together with one or more expansion modules.

Optional components for J100 IP Phone

You can use the following optional components with Avaya J100 Series IP Phones phones:

- PSAC12R-050 – 5V DC Power adapter
- JBM24 Button Module or Avaya J100 Expansion Module
- PoE power supply

Secondary display

Avaya J159 IP Phone and Avaya J189 IP Phone has a secondary display that is located at the lower right corner. It provides additional call appearances and feature or application display.

Secondary display has four pages with six lines per page, displaying 24 additional lines of information for incoming calls, outgoing calls, auto-dialing, and calling features. Use the left and right keys to navigate the pages.

Button modules

On 9600 Series IP Deskphones and Avaya J100 Series IP Phones, the number of call appearances and feature buttons can be extended with the JBM24 Button Module (JBM24) and the Avaya J100 Expansion Module (JEM24). The 9611G, 9608, 9641, and 9641GS each have a color display, and contrast adjustment is not applicable. All administered Button Module Labels, Call Appearances and Feature Buttons, display on the corresponding module buttons.

*** Note:**

The 9621G and J159 do not support a button module.

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

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

Avaya J189 IP Phone supports upto two expansion module (JEM24) and does not support JBM24 Button Module.

! Important:

Hot plugging is not supported in Avaya J100 Expansion Module. Connect all the expansion modules to the phone before connecting the phone to a power source.

The following table shows the number of button modules attached to the phone and the corresponding number of lines available on JBM24 Button Module / Avaya J100 Expansion Module:

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

*** Note:**

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

Chapter 3: Initial setup and connectivity

Installing the 9600 and J100 IP phones

Before you begin

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

Procedure

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

The phone powers up and starts to initialize.

3. The initialization procedure consists of the following processes:
 - a. The phone checks for LLDP messages.
 - b. The phone sends a DHCP DISCOVER message to discover the DHCP server in the network and invokes the DHCP process.
 - c. The phone verifies the VLAN ID, and starts tagging the data and voice packets accordingly.
 - d. The phone sends and identifies an upgrade script file, gets the `46xxsettings.txt` file, the language files, and any firmware updates.

If configured to use simple certificate enrollment protocol (SCEP), the phone downloads a valid device certificate.

4. Do one of the following:
 - To access the user login screen, press the **Login** softkey.
 - To access the craft menu, press **Mute** followed by craft access code (PROCPSWD), followed by **#**.

Related links

[Diagram: IP phone setup](#) on page 30

Prerequisites

Before deploying the product, ensure that you have the following knowledge, skills and tools.

Knowledge

- Networking
- H.323 protocol

Skills

Administering and configuring:

- Avaya Aura® Communication Manager
- DHCP server
- HTTP and HTTPS server

Tools

- Avaya Aura® Communication Manager
- Avaya Aura® System Manager

Hardware prerequisites

Ensure that the LAN:

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

Note:

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

Software prerequisites

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

- Avaya Aura® Communication Manager 6.3.6 or later
- Avaya Aura® System Manager 6.3.8 or later
- If applicable, IP Office IPO 11.0.0 or later
- A DHCP server for providing dynamic IP addresses to the Avaya J100 Series IP Phones.
- A file server, an HTTP, HTTPS, or the Avaya Aura® Utility Services for downloading the software distribution package and the `46xxsettings.txt` file

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

Avaya Aura® System Manager user profile worksheet

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

Data for	Field	Value	Notes
System Manager User Profile			
Identity tab			
	First Name		
	Login Name		
	Password		
	Localized Display Name		
	Endpoint Display Name		
	Language Preference		
	Time Zone		
Communication Profile tab			
Communication Profile section			
	Communication Profile Password		
Communication Address section			
	Handle Fully Qualified Address		
CM Endpoint Profile section			
	System		
	Profile Type		
	Use Existing Endpoints		
	Extension		
	Endpoint Template		
	Voice Mail Number		
	Conference server		
Messaging Profile section			Optional
	System		
	Mailbox Number		
	Template		
	Password		

Table continues...

Data for	Field	Value	Notes
	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		

Pre-installation checklist

Print copies of this checklist for each server and deskphone.

No.	Task	Notes	✓
Requirements for your network			
1	Your call server must have Avaya Aura [®] Communication Manager Release 6.2 or later version installed. Avaya only supports running on Communication Manager 6.2 or later.	-	
2	Verify that you have installed the following circuit packs on the switch: <ul style="list-style-type: none"> TN2602 or TN2302IP Media Processor circuit pack. Avaya recommends that sites with a TN2302 IP Media Processor circuit pack must install a TN2602 circuit pack to benefit from increased capacity. TN799C or D Control-LAN (C-LAN) circuit pack. ! Important: Release 6.0 or later requires TN799C V3 or greater C-LAN circuit pack(s).	-	
3	Verify that you have configured the Avaya call server correctly.	-	
4	Verify that you have administered the DHCP server and application correctly.	-	
5	Verify that you have administered the HTTP/HTTPS server and application correctly.	-	

Table continues...

No.	Task	Notes	✓
Requirements for your network			
6	Verify that you have loaded the upgrade script and application files correctly on the HTTP or HTTPS server.	-	
7	If applicable, administer the DNS server.	-	

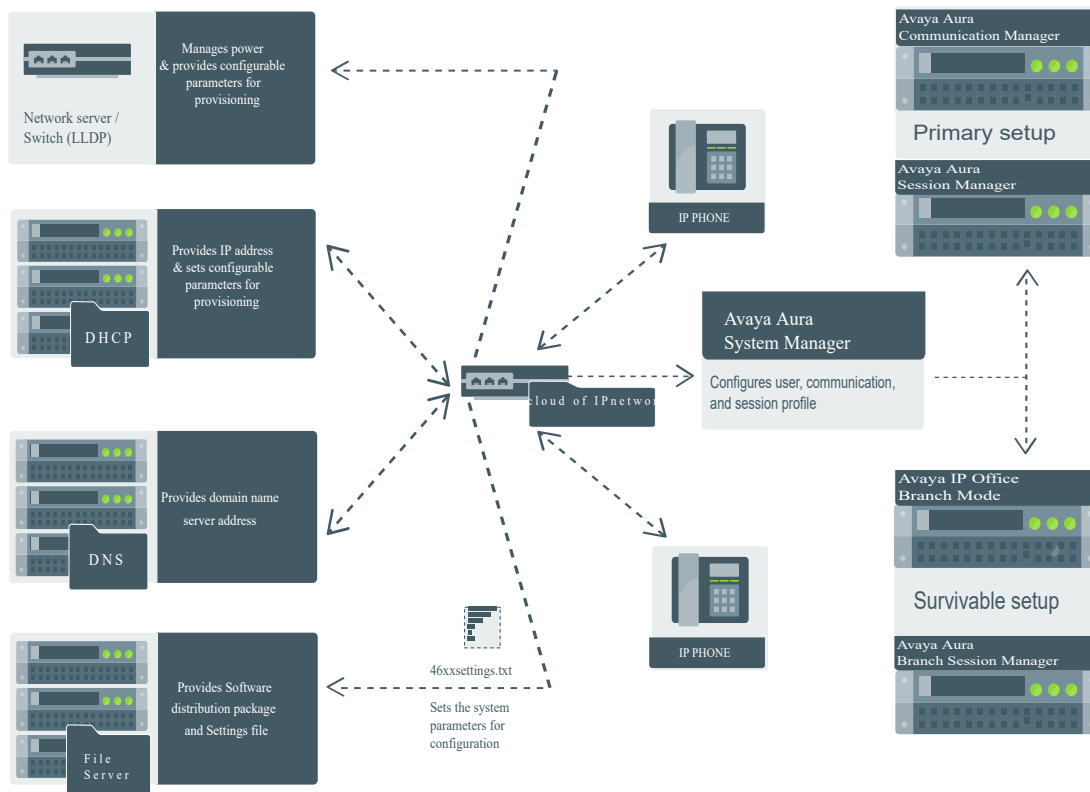
*** Note:**

All server applications, such as DHCP and DNS, can co-reside on the same hardware subject to the specific restrictions of each individual application.

No.	Task	Notes	✓
Requirements for each phone			
1	<p>Verify that you have an extension number and a Communication Manager security code (password) for each applicable IP phone. Without an extension or a password, the phone has limited functionality.</p> <p>* Note:</p> <p>If your call server and the <code>46xxsettings.txt</code> file support unnamed registration, you do not need an extension or password.</p>	About unnamed registration on page 47	

For more information, see Communication Manager documentation on the [Avaya Support website](#).

Diagram: IP phone setup

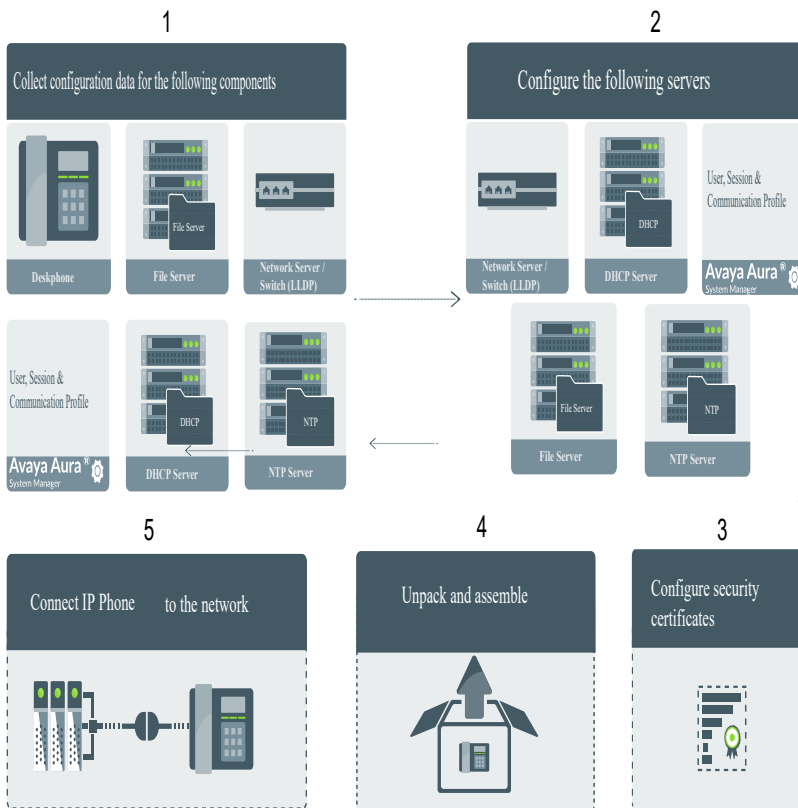


Related links

[Installing the 9600 and J100 IP phones](#) on page 25

[Diagram: Phone deployment process](#) on page 31

Diagram: Phone deployment process



Related links

[Diagram: IP phone setup](#) on page 30

Upgrading the phones

Updating phone software for installation

About this task

A phone that is shipped from the factory might not contain the most up-to-date software for registration and operation. When you first plug in the phone, a software download from an HTTP server might be initiated. The software download provides the phone upgraded functionality.

For subsequent downloads of software upgrades, the Avaya call server provides the capability for a remote restart of the IP phone. When you restart the phone, the phone automatically restarts and performs a download if new software is available. For more information, see [About software distribution packages](#) on page 225 and [Downloading software packages](#) on page 226.

Plugging in the IP phones

About this task

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.

Avaya J100 Series IP Phones supports the IEEE 802.3af-PoE power supply along with an additional 5V power adapter.

You can only provide power to the 9608, 9608G, 9611G, 9621G, 9641G and 9641GS deskphones 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.

Note:

Avaya J100 Series IP Phones does not support the Global Single Port PoE Injector (GSPPOE-xx).

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.

Table 1 below 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 or the 9600 series phones. When you add USB devices, the deskphone displays instructions for any additional power needs.

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:

Avaya J100 Series IP Phones does not support the Dual Headset Adapter (DHA).

Avaya J159 IP Phone is a PoE class 1 device and does not support any button module or a USB device.

9608G do not have Gigabit Ethernet LED

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

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

*** Note:**

Power specifications for J100 Series IP Phones specifies the power requirement of the J100 series phones as per the connected peripherals.

The deskphone monitors power consumption to conform to the IEEE 802.3af specifications. If you connect a Dual Headset Adapter (DHA) to the 9600 series IP Phone, the power classification might change and you must then change the switch setting as well.

In J189, 9611G, 9641G, and 9641GS, the USB interface supports USB login, use of digital pictures from a USB device as a screensaver, and import or export of contact lists by a Flash drive. Since the power consumption of the drive varies from product to product, you cannot state how a USB will impact PoE power class. When the drive attempts to register with the deskphone, the deskphone determines if its current power class setting is adequate to support the drive. If power is adequate, the deskphone lets the drive register. If the power is not adequate, the deskphone will alert the user to change the power class by changing the IEEE power switch setting from L to H. In extreme situations, the total power consumption with the addition of a USB device may be greater than what the Class 3 power source can provide. In that case, the deskphone detects this and instructs the user to use an auxiliary power supply or to temporarily disconnect one or more of the modules while the USB device is in use. The system parameter USBPOWER determines for which power class or classes to enable power to the USB interface.


The last step in assembling the 9600 Series IP Deskphone and Avaya J100 Series IP Phones 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).

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 9600 series deskphones:

Deskphone Model:	See figure:
------------------	-------------

Table continues...

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

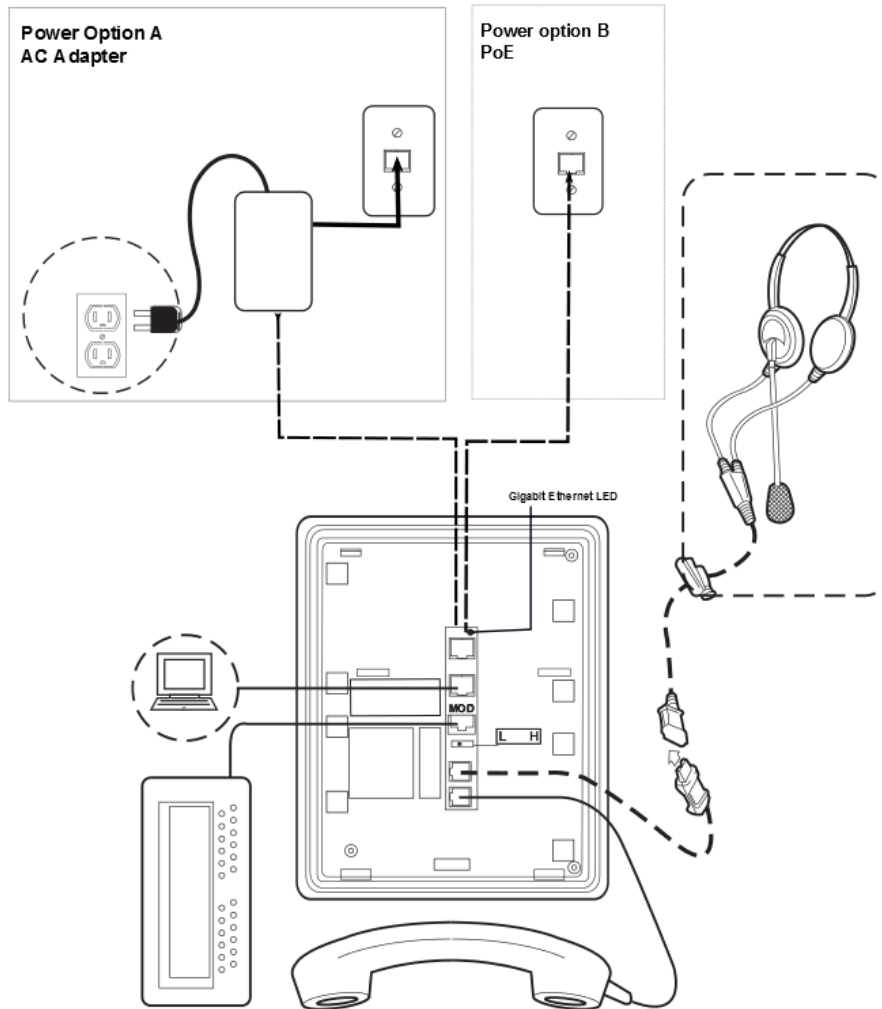
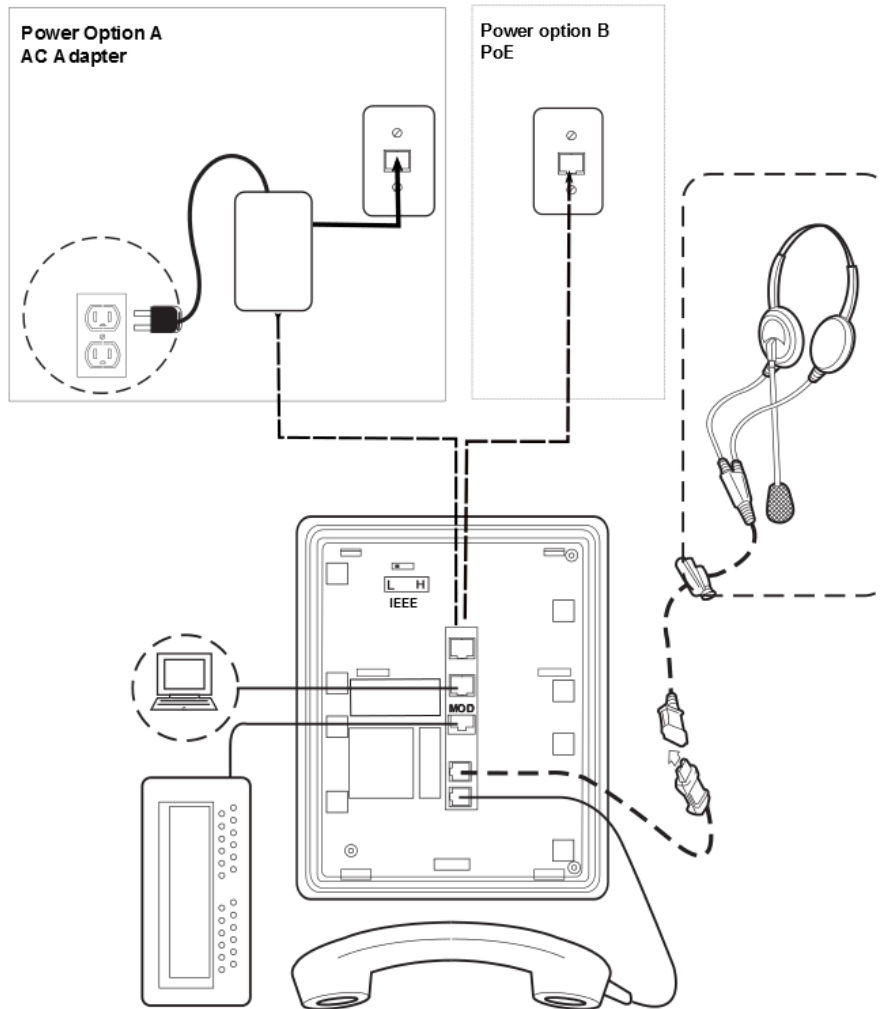


Figure 1: Connection jacks on a 9608, 9608G, or 9611G deskphone

*** Note:**

The Gigabit Ethernet LED indicator is applicable to 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.

Completing the power connection for 9600 Series Deskphones

Procedure

1. Plug one end of the H4DU 4-conductor coiled handset cord into the phone and the other end into the handset.
2. Plug one end of the first Category 5 modular line cord into the Ethernet jack of the PC and the other end into the secondary Ethernet jack on the phone, if appropriate.
3. For an IEEE-powered deskphone, plug one end of the second Category 5 modular line cord into the Ethernet jack on the phone. Plug the other end of this cord into the Ethernet wall jack.
4. For a locally powered deskphone, connect the Category 5 modular line cord provided with the IP Phone Global Single Port PoE Injector GSPPOE-xx, where xx represents the model number into the Ethernet jack on the phone. Plug the femite end of this cord into the deskphone. Plug the other end of this cord into the GSPPOE-xx power injector jack labeled **DATA & POWER OUT**. Plug another Category 5 cord into the GSPPOE-xx power injector jack labeled **DATA IN**. Plug the other end of this cord into the Ethernet wall jack. Finally, connect the GSPPOE-xx to an AC power source.

Installing a Dual Headset Adapter (DHA)

About this task

You can install Dual Headset Adapter (DHA) on call center deskphones for 96x1 models except 9621G . The supervisor can monitor calls in progress by attaching a DHA directly to a deskphone or to an attached button module.

Order the 96x1 Dual Headset Adapter Kit (PK25) (Comcode 700500729), which includes dual headset adapters and required cables for 25 deskphones.

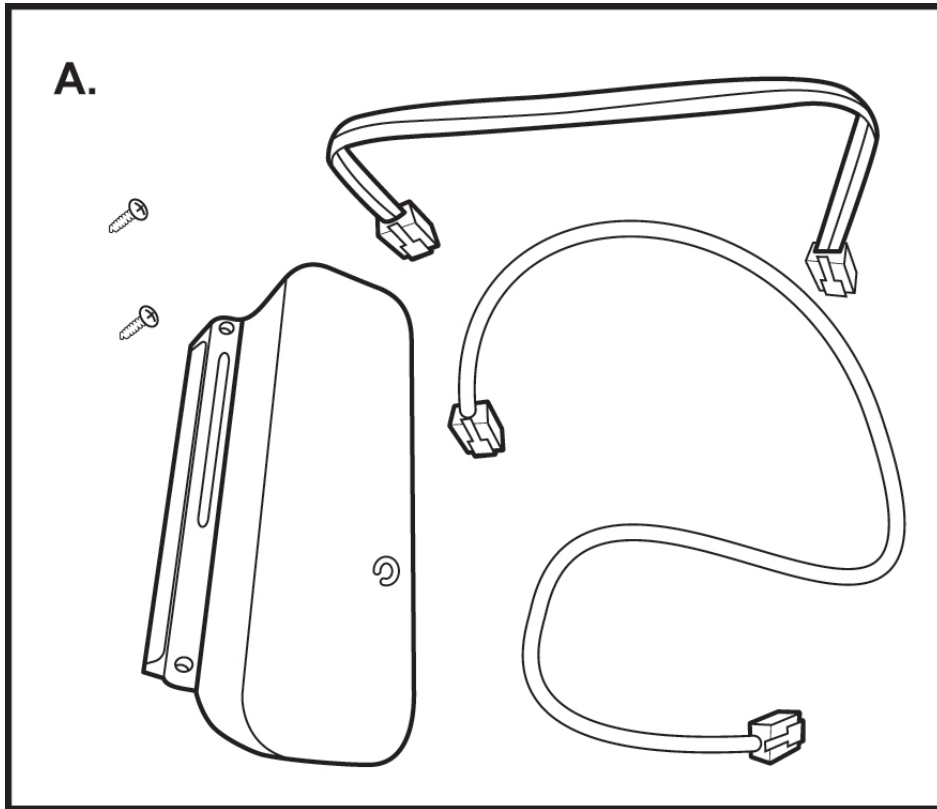


Figure A shows the DHA Package Contents.

To install a DHA directly to the deskphone and alternatively to an attached button module, see the following figure.

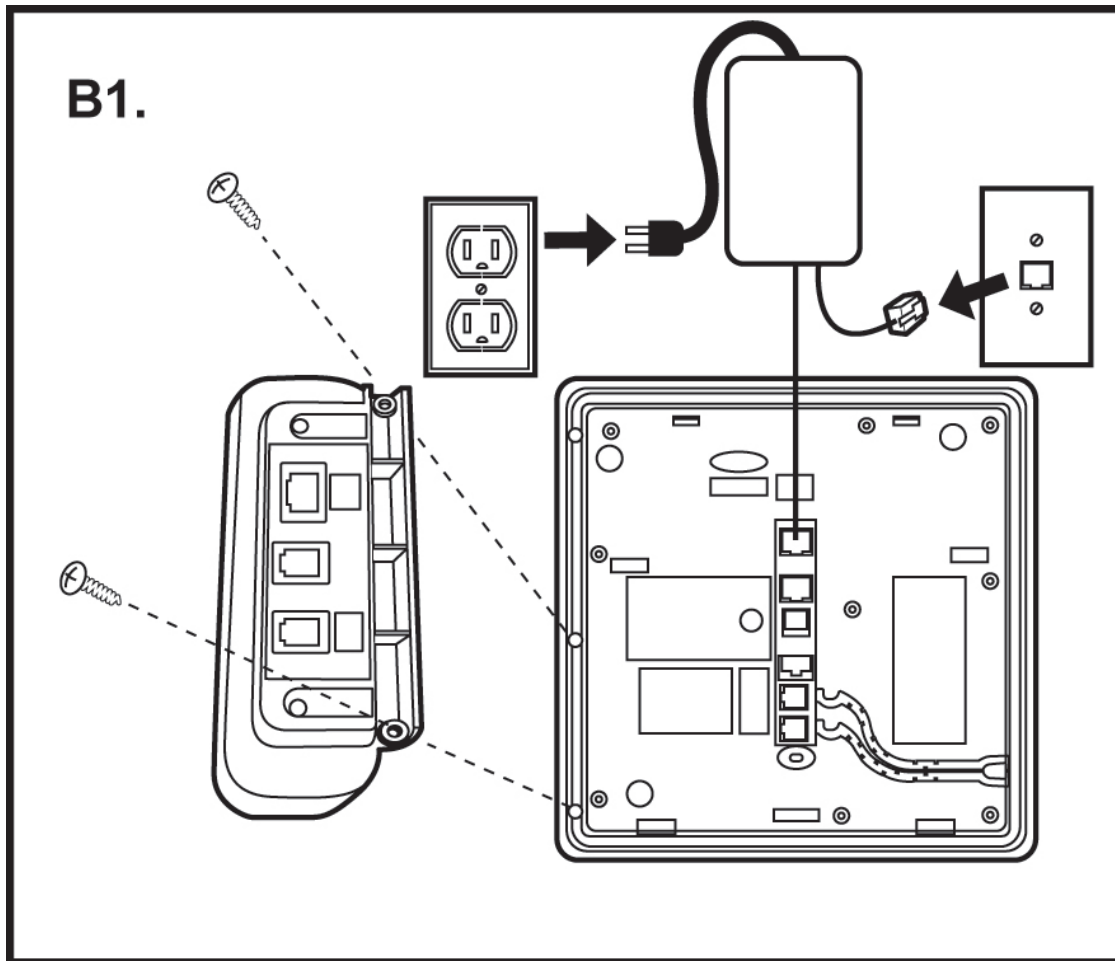


Figure B1 :Attaching the DHA to a deskphone.

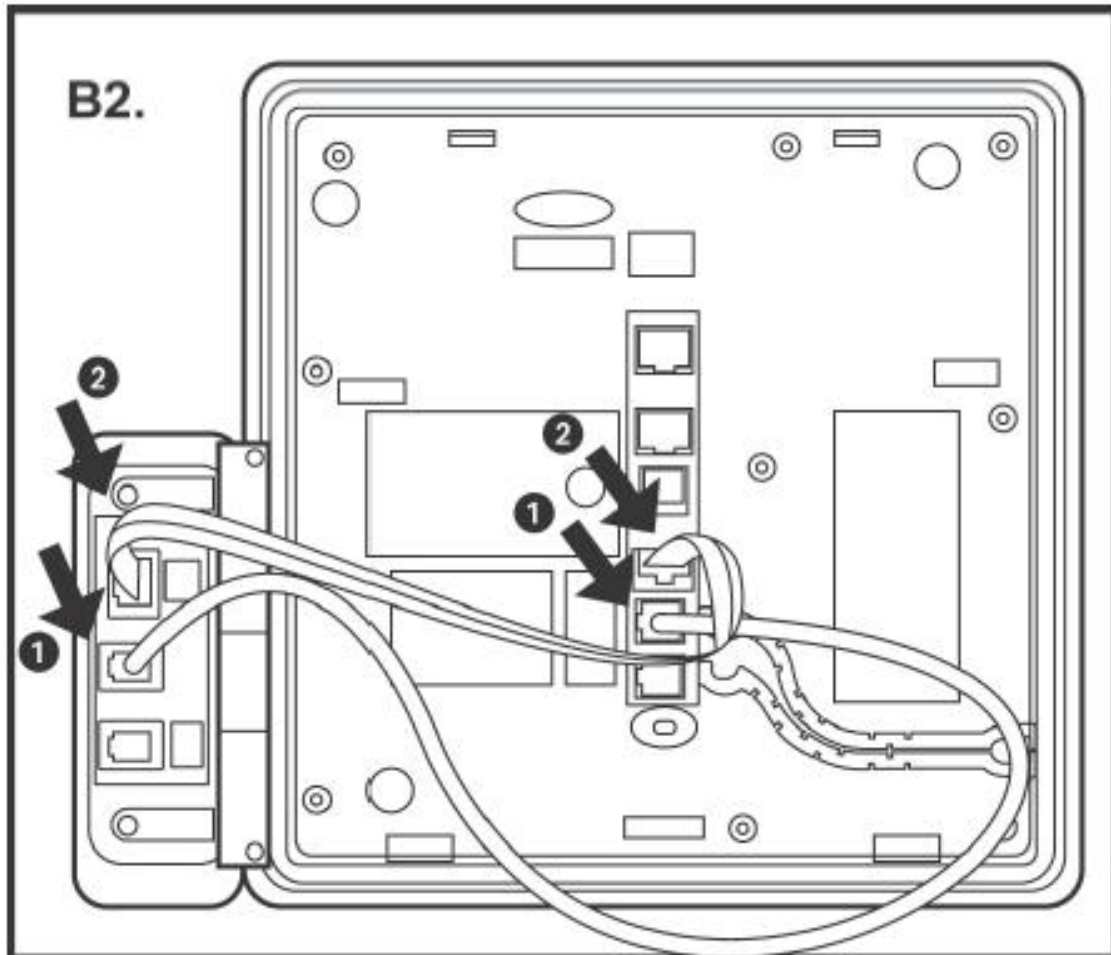


Figure B2 : Attaching the DHA to the phone power and audio cables.

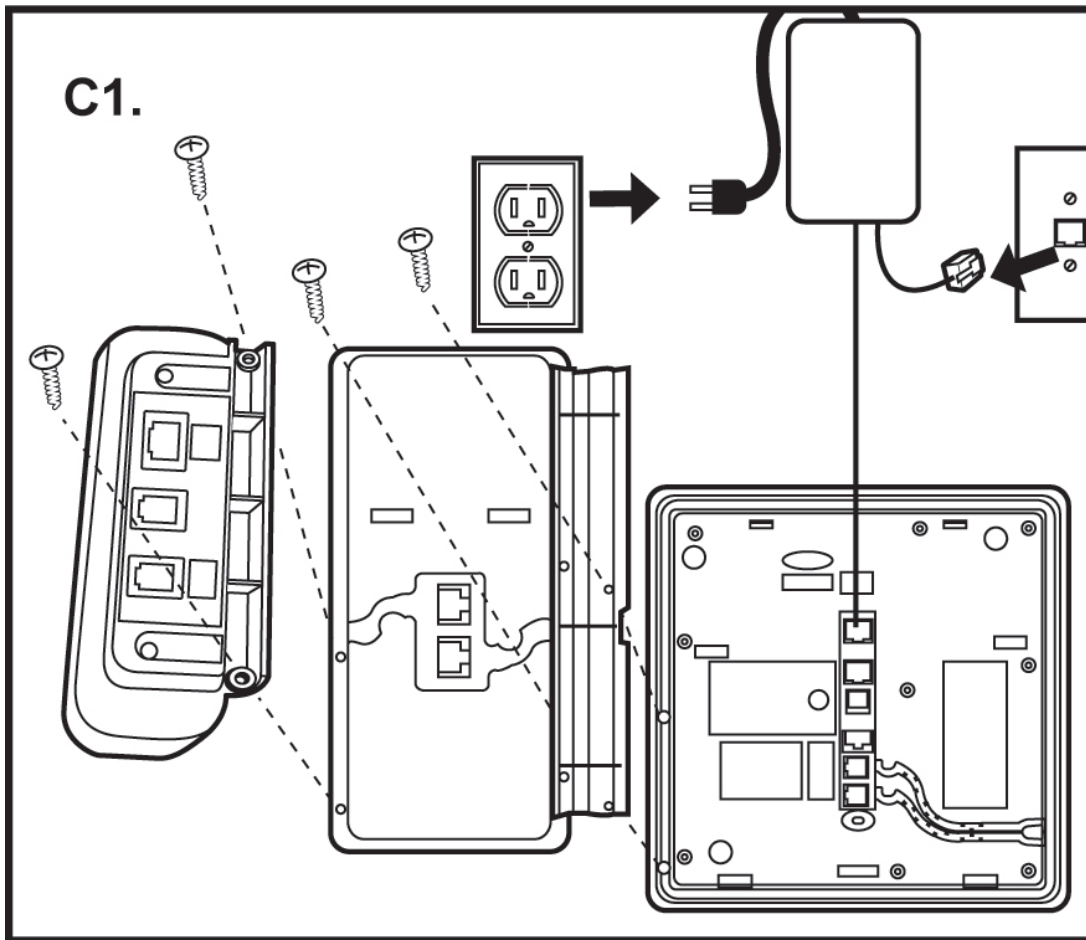


Figure C1: Attaching the DHA to an (optional) button module.

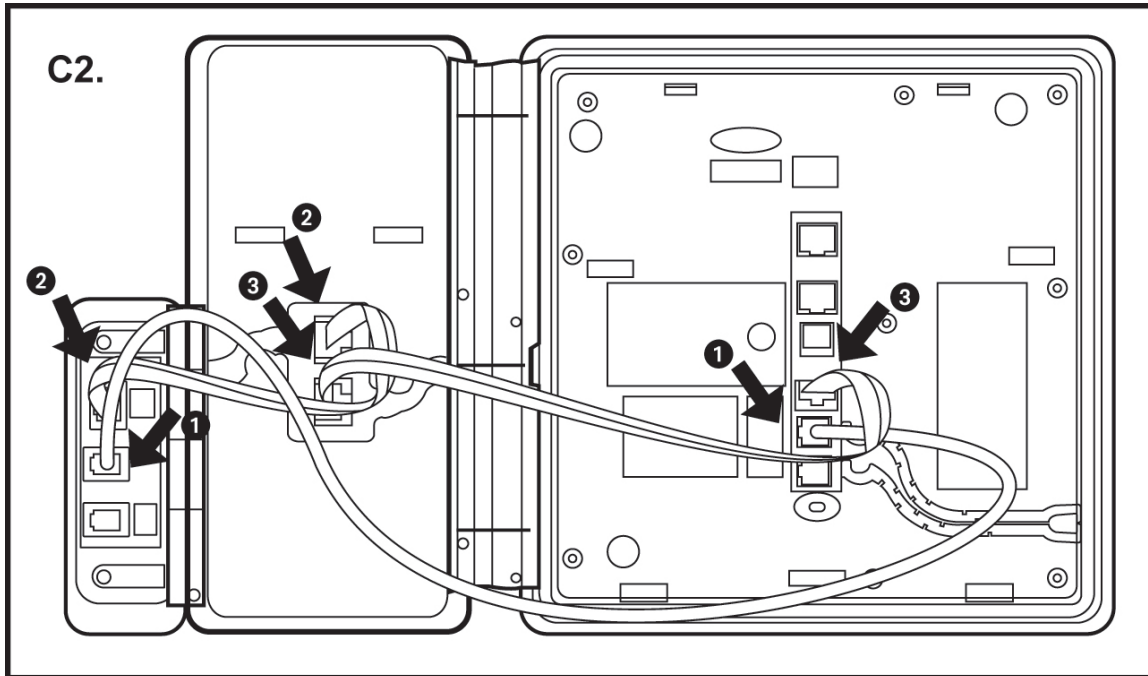


Figure C2: Attaching cable connection of the DHA to an optional button module and the deskphone.

Installing 9641G Call Center faceplate

About this task

The 9641G IP deskphones used in a call center come with special faceplate kits: 9641G Call Center Faceplate Kit (PK25) (Comcode 700500728). The removeable faceplate has the following features:

- Covers the handset pockets
- Maintains the switch hook “down” position
- Covers the **Forward** and **Headset** buttons
- Relabels the **Speaker** button as the **Release** button to facilitate ending calls

* Note:

To allow **Release** button operation for 9641G deskphones, administer the **Release** button with the AGTSPKRSTAT parameter set to 2 and the CALLCTRSTAT parameter set to 1.

Procedure

1. If already connected, remove the HAC cord from the underside of the phone.
2. With the phone facing up and resting flat on a hard surface, pry up a corner of the standard faceplate until the faceplate is released from the phone.

You can use your fingers, a flat screwdriver, or other non-sharp device to pry around the edge of the standard faceplate.

3. Align the tabs on the 9641G Call Center faceplate with the slots on the outer edges of the deskphone and push down to lock the tabs into the slots.
4. Ensure that the display bezel surrounding the screen is in proper position.
5. Plug the HAC cord back into the underside of the phone.

Plugging in and resetting the phones using the Dynamic Addressing Process

Note:

Before you start this process, you must have an extension number for the IP phone and the Communication Manager security code (password) for that extension, unless you intend to use the deskphone with unnamed registration. Any reference to an HTTP server applies equally to an HTTPS server. You can plug in and reset the phone successfully using the following description.

As the phone initializes, you will see messages, some of which are part of DHCP process, with a power on indication and dynamic feedback. These messages indicate that the phone is active and not locked. You will also receive useful information, about the status of the network, the server, or the downloading operations, before the dial tone.

Understanding the plug in and reset process

Plug the phone into the Ethernet wall jack. The phone receives power from the port and performs the following processes:

Note:

Do not unplug the phone during the download process. Wait for the download process to complete. If the application was downloaded earlier, the whole process takes approximately 1 to 2 minutes after the phone is plugged in. For software upgrades, including the boot file and application file download, the process might take 5 to 10 minutes. The duration depends on factors such as LAN loading and the number of phones being installed.

During hardware initialization, the system initialization values NVCONTRAST and NVBRIGHTNESS are checked for non-null values, and set accordingly. phones with bit-mapped display screens show the Avaya IP phone name and logo.

1. The system checks the system initialization value for the language file in use (NVLANGFILE) for a non-null value, in which case the text strings in that language file are used for text display. Otherwise, the display shows English text strings.

2. The boot programs check the Kernel or the Root File System that has previously been marked as the one to be activated to ensure that it has not become corrupted. If the Kernel or the Root File System is not corrupted, the system transfers control to a process in that file system. If that file system is corrupted, the boot program checks the other Kernel/Root File System. If that file system is not corrupted, the file system is marked as the one to be activated. The system then sets the value of RFSINUSE to the name of the Signed Kernel or Root Software Package that was used to install that file system, and the control is transferred to the Signed Kernel or Root Software Package. If both Kernel and Root File Systems are corrupted, the system halts the processing. The software checks whether a Signed Application or Library Software Package has been previously downloaded. If the system finds the Application Software Package or the Library Software Package the Application Software Package or the Library Software Package is installed. If either the Application Software Package or the Library Software Package has a different file name than the currently installed version, the system replaces the existing corresponding files in the Application File System. The system then deletes the downloaded Signed Application or Library Software Package. If a new Signed Application or Library Software Package is not found, the integrity of the application files is checked. If the files are corrupted, the system installs the files from the Backup Package, replacing the corrupted files in the Application File System. Each time an Application Software Package or a Library Software Package is installed, the system sets the value of the persistent parameter APPINUSE to the file name of the Application Software Package that was installed. If the application files are not corrupted, or after the Backup Package has been installed, control is transferred to the application installed in the Application File System. While the system loads the application files into volatile memory and transfers control is transferred to the application files, the bottom text line shows the value of the APPINUSE parameter.
3. The system starts and sets the internal clock/calendar is set to 0:00:00 Saturday, January 1, 2000.
4. The phone activates the Ethernet line interface , the PC Ethernet jack, and dial pad input to allow the start of procedures. The activation occurs soon after power-up or a reset.

The phone displays the speed of the Ethernet interface in Mbps, that is, 10, 100, or 1000. The phone then displays the message `No Ethernet * to program` until the software determines whether the interface is 10 Mbps, 100 Mbps, or 1000 Mbps.

 **Note:**

The Ethernet speed is the LAN interface speed for both the phone and any attached computer, if the administrator has not disabled the latter interface by a PHY2STAT setting.

 **Important:**

When you press the star (*) after the system displays a `* to program` message. The initialization process can support an interrupt that invokes the Craft Access entry procedure to allow manual settings, only if the local dialpad procedure status (PROCSTAT) system value is 0. The zero PROCSTAT value provides full access to local procedures. If PROCSTAT is 1 the Craft Access entry procedure can be invoked

only when a `* to program` message displays, but only the VIEW procedure is available.

5. The IP phone sends a request to the DHCP server and invokes the DHCP process.

The phone displays one of the following messages:

- DHCP: `s secs * to program`
- DHCP: `s secs VLAN ID = n`

where *s* is the number of seconds that have elapsed after the DHCP process was started. The phone displays the first message if 802.1Q tagging is off and access to local programming procedures is not disabled or restricted. The phone displays the second message if 802.1Q tagging is on and access to local programming procedures is disabled or restricted. If the first and second message alternate every 2 seconds, 802.1Q tagging is on. When the phone displays both messages alternately, access to local programming procedures is not disabled or restricted.

6. The system determines the DHCP protocol, IPv4 or IPv6 protocol, and the applicable parameters that are enabled.

 **Important:**

IPv6 operation is limited to a specific customer set and not for general use.

 **Note:**

The IPV6STAT parameter overrides both the DHCPSTAT parameter setting and manual programming.

The DHCP server provides the IP addresses for the following hardware:

- The phone
- The HTTP/HTTPS server
- The TN799C or D Control-LAN (C-LAN) circuit pack on the media server

7. Using the list of gateway IP addresses provided by the DHCP server, the phone performs a router check. The phone cycles through the gateway IP addresses with ARPs or pings until it receives a response. When the router is located, the router processes the received LLDP TLVs. Then the HTTP process starts.
8. While the IP phone connects to the HTTP server, the phone displays one of the following messages:

HTTP: `n ipadd`

or HTTP: `n ipadd * to program`

or HTTP: `n ipaddProgram`

where *n* is the number of the IP address obtained from the HTTP server and *ipadd* is the IP address.

! Important:

Pressing star (*) at this time invokes the Craft Access entry procedure to allow manual settings.

9. When connected, the phone looks for an upgrade script file.

10. The HTTP server sends and identifies an upgrade script.

The phone might send the GET message several times. Each time the GET message is sent, all IP phones display the following message: `HTTP: n uri`

For HTTP, *n* is the number of HTTP requests made by the phone and *uri* is the URI for the current HTTP request.

*** Note:**

The SIG parameter value determines the signaling protocol whether H.323 or SIP, and is used to determine the proper upgrade file that is downloaded. If you set the SIG parameter manually using the local administrative Craft SIG procedure, that value takes precedence over a SIG setting in a configuration file. A change in the SIG value might require a reset to the phone so that a new or different upgrade file can be downloaded to the phone.

11. While the upgrade script file is being downloaded, all IP phones display the following message: `HTTP: n sc etag`

where *n* is the number of the IP address obtained from the HTTP server, *sc* is the status code of the HTTP response, and *etag* is the value of the ETag header.

12. When the phone establishes the validity of the application file received, the phone displays the following message: `File Obtained; please wait..... s secs`

where *s* is the number of seconds that elapse while non-volatile memory is erased.

13. While the application file is saved in flash memory, all IP phones display the following message: `Saving to flash 1% 1 secs`

where the percentage of the file and the number of elapsed seconds increase as the application file is stored in flash memory.

14. The phone contacts the Avaya Communication Manager and displays a login screen that displays the following:

`Login, Enter Extension, or Enter Extension and press Enter or OK.`

Steps to be performed by user after phone displays login and extension prompts:

1. Enter a new extension and press **OK**.

*** Note:**

Unnamed registration is registering a phone with the call server without entry of an extension or password. You must set the UNNAMEDSTAT parameter to enable unnamed registration. The phones that are registered unnamed have limited functionality.

All IP phones display the following:

```
Login
Enter Password
Enter Password and press Enter or OK
```

2. To register the phone without the extension or password (unnamed), press **Log In** or make no entry and wait 60 seconds.

You can see the extension as you enter the extension, but the password is displayed as stars (*). The system determines whether the extension is in use.

 **Note:**

The phone stops at the discovery mode in the following conditions:

- The login credentials are incorrect.
- The phone is logged in but one of the gatekeepers is not reachable because of an upgrade or a network outage. In the discovery mode, press **Reset**. The phone deletes the credentials from the memory, reboots, and displays the Login page.

In the registration mode, the phone restarts, but it does not delete the login credentials.

When this process is complete, you can hear a dial tone when you press the **Speaker** button or lift the handset. The dial tone indicates that the IP phone was installed successfully.

Understanding Unnamed registration

In an IP phone, when you register with a call server, and receive limited service, without requiring an extension and password entry, this functionality is called as Unnamed registration. Unnamed registration is useful in the following environments:

- “Hot-desking” environments where a time gap exists between one user logging out and another user logging in on the same deskphone.
- Road warrior mode of use where a traveller can run the telephony features and functionality by taking over the office deskphone extension.

In both examples, the user unregisters the deskphone by logging off or by taking the office deskphone extension over to another deskphone. Without Unnamed registration, the deskphone in the first example will wait for an extension and password entry and the deskphone in the second example will continue attempting to register at regular intervals. The disadvantage of a unregistered deskphone is that no one can use the deskphone, for example, to report a building emergency like a fire.

In Unnamed registration, the deskphone registers without an extension and password. Because there is no extension, telephony functionality is limited, specifically:

- The user has only one call appearance, and hence, cannot transfer or conference calls.
- The user has no administered feature buttons, and cannot invoke on-hook dialing.
- The user cannot reach extension-based information, such as the Contacts data of a given user or Option settings.
- The user is limited to the calling capability administered for PSA (Personal Station Access) on the call server, for example, access to an emergency number.
- The deskphone cannot receive any outside calls.

Unless otherwise disabled, the deskphone automatically attempts to register unnamed if no action is taken on the deskphone extension entry screen within 60 seconds. To disable and prevent Unnamed registration, enter an ID or password. The system ignores Unnamed registration after any dialpad entry.

Administrators can disable Unnamed registration by appropriately administering the system parameter UNNAMEDSTAT. Unnamed registration appears to the end user like Communication Manager TTI Mode and is similar from an administration perspective. For more information about TTI, see your Communication Manager documentation.

Wall mounting Avaya J100 Series IP Phones

About this task

The wall mount kit is not bundled with the phone package. You must separately purchase the wall mount kit that is unique to your phone model. Use the following part number to order the wall mount kit:

- J159, J169, J179, J189 phones — 700513631.

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

Before you begin

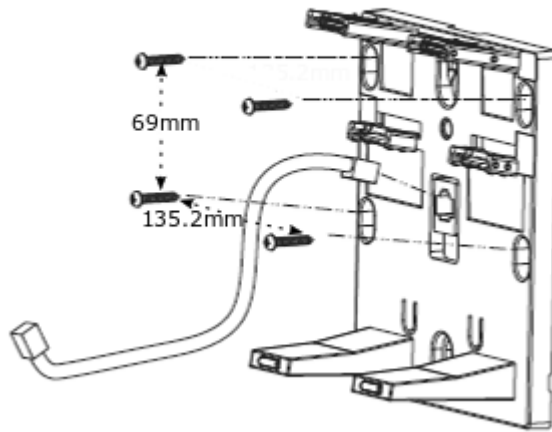
Obtain the following items:

- Wall mounting kit, containing a wall mount bracket, and an Ethernet cable.
- Four #8 screws. The screws are not provided with the wall mounting kit. If the wall plate is pre-installed, you do not need the screws.

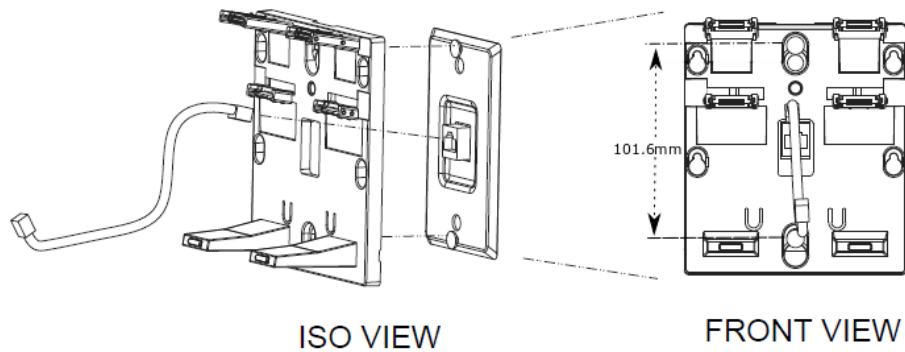
Procedure

1. Do one of the following:

- Place the bracket on the wall and mark to drill holes. Use four #8 screws to fix the bracket.

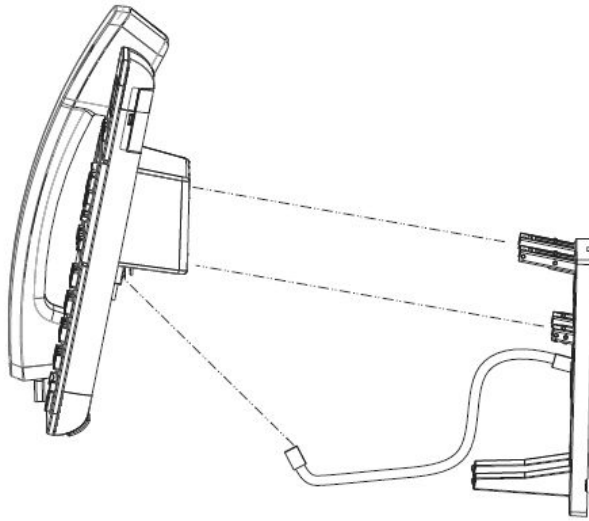


- If the wall plate is pre-installed, fit the wall mount bracket over the wall plate.



2. Connect one end of the Ethernet cable to the network port of the phone and the other end to the wall jack.
3. To attach the phone to the wall mount bracket, insert the two upper tabs of the bracket into the slots on the back panel of the phone.

The lower pair of tabs rest against the back panel. The phone does not move when you press a key on the phone.



Wall mounting Avaya J100 Expansion Module

About this task

If your phone is wall mounted, you must additionally install the wall mount for the Avaya J100 Expansion Module. You must separately purchase the wall mount for the expansion module. The part number of the wall mount kit is 700514338.

Before you begin

Obtain the following items:

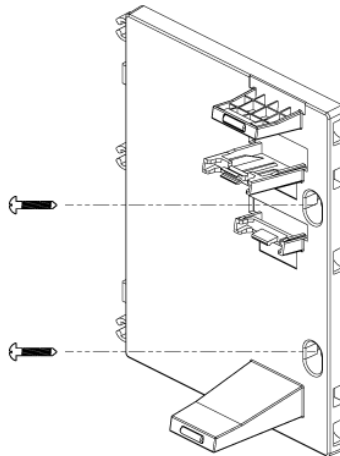
- Wall mount kit, containing a wall mount bracket.
- Two #8 screws. The screws are not provided with the wall mounting kit.
- Link for connecting expansion module for Avaya J189 IP Phone that comes along with the kit.

Procedure

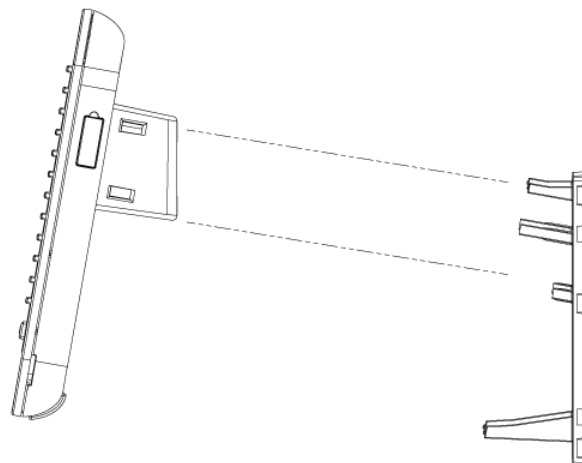
1. Remove the phone from the wall mount.
2. Place the expansion module bracket on one level to the right of the phone bracket, mark and drill holes, and then affix the #8 screws.

Note:

Use the link for installing wall mounting kit of Avaya J189 IP Phone.



3. To attach the Avaya J100 Expansion Module to the wall mount bracket, insert the upper tab of the bracket into the slot on the back panel of the expansion module.



4. Connect the expansion module to the phone as one assembled unit.
5. Connect the ethernet to the assembled unit.
6. Attach the phone to the wall mount bracket.

Local Administration menu procedures

During or after you successfully install an IP phone, a system message might instruct you to administer one of the manual procedures described in this chapter. These local administrative procedures are also referred to as Craft procedures.

Local administrative options have two forms. One of them provides access to all the capabilities and functions described in this chapter.

The other provides access only to the administrable level of VPN capabilities and functions.

Using the VPN-specific option, the administrator can grant VPN users access to the VPN procedure itself, while preventing these users from gaining access to any other local administrative procedure. The administrator may grant the VPN user permission to change VPN settings or only to view the settings.

If the PROCSTAT is 0, you have full access to local Craft procedures and you can invoke local craft procedures during initialization or whenever the deskphone displays this message:

```
* to program
```

You can also initiate the Craft procedure at any other time the initialization process can support a processing interrupt. If you set PROCSTAT to 1, the system allows access only to the VIEW craft procedure for debugging purposes. You can invoke local Craft procedures only when the “* to program” message displays during initialization.

The factory-set default Craft Access Code (PROCPSWD) is **27238**. This default PROCPSWD code should be replaced by the administrator.

Caution:

Only trained installers or technicians should perform local administrative 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 with static administration of these options than by dynamic administration. Values assigned to options in static administration do not change with upgrade scripts. These values remain stored in the phone until one of the following happens:

- You download a new boot file.
- You reset the IP phone.

Related links

[Running Craft procedures](#) on page 53

[Accessing the Administration menu after phone startup](#) on page 54

[Entering data for administrative options](#) on page 54

[Entering and validating IPv4 and IPv6 addresses](#) on page 55

[Local administrative Craft procedures menu](#) on page 57

[Setting the operational mode to 802.1X](#) on page 58

[Changing IP address information](#) on page 59

[Clearing the phone settings](#) on page 61

[Debug mode](#) on page 62
[Changing Ethernet interface control](#) on page 63
[Disabling and enabling event logging](#) on page 64
[Logging off from the phone](#) on page 65
[Viewing multilanguage strings](#) on page 66
[Resetting system values](#) on page 66
[Restarting the phone](#) on page 67
[Setting or changing the signaling protocol](#) on page 67
[Changing SSON settings](#) on page 68
[Performing a self-test](#) on page 69

Running Craft procedures

About this task

Follow the steps for running the Craft procedure.

* Note:

The administrator may allow access to only the VPN procedure, by setting the VPNCODE parameter in the `46xxsettings.txt` file. For more information on access to VPN-only Local Administrative Options, see *VPN Setup Guide for 9600 Series IP Telephones*.

* Note:

The system supports the * to program message even if the value of PROCSTAT is 1, when the messages Address conflict, Subnet conflict, Bad router? and Bad FileSv address display. You can gain execute the Craft procedures in response to these messages as the situations requires corrective input.

Procedure

1. Press * to display the Craft Access Code Entry screen during deskphone startup and start local procedures.

```
Enter code: __
# = OK
```

2. Enter the password and press # or **OK**.

For security purposes, the deskphone displays a star (*) for each numeric dialpad press. You can use the left arrow button or the designated softkey for non-touch screen phones.

The entry is compared to the PROCPSWD value. If they match, the deskphone displays the Craft Local Procedure screen, and the message Select procedure and press Start.

3. For all IP phones, use the navigation arrows to scroll to and highlight the local procedure you want, then press **Start** or **OK**.

You can also scroll to the procedure you want and press the corresponding line button.

Related links

[Local Administration menu procedures](#) on page 52

Accessing the Administration menu after phone startup

About this task

The administration menu in the phone can only be accessed by craft menu.

Procedure

To access the craft menu, press **Mute** followed by craft access code (PROCPSWD), followed by #.

Related links

[Local Administration menu procedures](#) on page 52

Entering data for administrative options

About this task

This section applies to all IP deskphones and describes how to enter data for administrative options.

Procedure

1. The first application line on any screen is automatically highlighted selected when the phone displays the screen. To select an item, press one of the following softkey.

- **Change**
- **Save**
- **Start**
- **OK**

Note:

The deskphone emits an error beep if you attempt to enter invalid data.

2. To select a different line, use the down or up navigation arrows to change the line focus. When the desired line is highlighted, then press a softkey or **OK** to select that line.
3. If you enter a numeric digit that exceeds the maximum field value of the IP Address or subnet mask value, that is exceeds 255, the phone emits an error beep tone. The system ignores the digit, and the cursor does not move forward.
4. If you enter a zero followed by a numeric digit for a value, an IP Address, or a subnet mask field, the new digit replaces the zero.

If you press star (*) and enter an IPv4 address, the system inserts a decimal point into the input buffer and moves the cursor to the next character location. If the star (*) button is

pressed and the user is entering an IPv6 address, the system inserts a colon into the input buffer and the cursor is moved to the next character location.

5. To go back to previous screen , press the left most softkey.

When you press the applicable button or key to backspace, the most recently entered digit or period is erased from the display. The cursor remains in the erased character's former position.

6. Press **Exit** to exit the local procedures.

 **Important:**

If any changes were made using the 802.1X procedure or the ADDR procedure, if the value of SIG was changed to SIP or if the Crafts Entry screen was invoked during startup, the deskphone immediately resets when you press or touch **Exit**. If no 802.1X, SIG, or ADDR changes were made, or if the local procedures were invoked post-startup, the deskphone redisplay the screen or other display that was effective when the craft options was invoked.

 **Note:**

If PROCSTAT has been administered to 1, you will not be able to invoke any administrative options other than VIEW.

Related links

[Local Administration menu procedures](#) on page 52

Entering and validating IPv4 and IPv6 addresses

The dial pad uses numeric-only entry when an IPv4 address or the subnet mask is entered. Use an asterisk to place a period within the address being entered.

When you press star (*) on the dial pad with the cursor in one of the three fields towards the left of the display, the following happens:

- The field where you are trying to enter a value displays a zero if no value is entered.
- If you enter a valid value a period displays. The space after the field displays a period.
- The cursor moves to the next space.

When you press star (*) with the cursor in one of the three fields to the right side of the display, the system beeps to indicate an error and the cursor remains in the field to the right. Pressing the "*" button while the cursor is in the last (right most) field results in an error beep and the cursor being left where it is. If you enter all three dots that separate the fields and if the value of each field is valid, the IPv4 address or subnet mask is complete.

The value of a given field might be invalid when you:

- Enter a digit that makes the value of the first field of an IPv4 address exceed 255.
- Enter a digit that makes the value of the last three fields of an IPv4 address exceed 255.

- Enter a digit that makes the value of any field of a subnet mask exceed 255.

Enter an IPv6 address using only numbers on the dial pad. When you press 2 the deskphone initially enters a 2, followed by A, B, C, and back to 2. When you press 3 the deskphone initially enters a 3, followed by D, E, F, and back to 3. While the cursor is in any of the left most seven fields, when you press the star (*) button makes the value for the field being entered to be terminated (a zero is displayed if nothing else is), a colon to be displayed in the space after the field, and the cursor to move to the next space. Pressing "*" while the cursor is in the last (right most) field results in an error beep and the cursor being left where it is. An IPv6 address is considered to be complete only if all the following conditions are met:

- All seven colons that separate the fields are entered OR the text input field contains at most one pair of consecutive colons
- If one pair of consecutive colons is present, the final field is not "1" or "01".
- If one pair of consecutive colons is present, the address format is not "::FFFF:hhhh;hhhh".
- The value of each field is valid. The following actions cause the value of a given field to be considered invalid:
 - Entering a digit that would cause the value of the first field of an IPv6 address to exceed FD.
 - Entering a third consecutive colon.
 - Entering a second pair of consecutive colons.

In a given text entry field, if the either an IPv4 or an IPv6 address can be specified, the initial field can be ambiguous with respect to whether the entry is an IPv4 or IPV6 address, for example, 123 might be an IPv4 *123 decimal* or an IPv6 *0123 hex*. In such cases, text entry follows the IPv6 rules that hexadecimal characters are allowed and the "*" key inserts a colon character. If the entry is a hex character (A-F) or a fourth character is entered in the field, the telephone accepts the input is IPv6 format. Otherwise, the telephone makes the initial validity check when you enter a field boundary, a colon or decimal point. This initial typographic character determines whether the overall address must be in IPv4 format with a decimal point or in IPv6 format with a colon. Once this character is entered, the telephone examines the contents of the first field to ensure consistency with the field boundary. That is the absence of hex characters, and at most three characters of value 255 or less, in the first field if the field boundary is a decimal point. If the first field contains any content inappropriate for the entered field boundary, an error beep is generated. You cannot enter more content until the contradiction in the text string is deleted, meaning either the field boundary is deleted or the cursor is moved back and the field contents edited). After you enter content that identifies the format of the IP address appropriate to IPv4 or IPv6, the rest of the address entry conforms to that format.

Related links

[Local Administration menu procedures](#) on page 52

Local administrative Craft procedures menu

Using the administrative procedures, you can customize the IP deskphone installation for your specific operating environment. This section provides a description of each local administrative option covered in this guide, with references to the pages on which the option appears.

*** Note:**

You should press a line key to select a line. Depending upon the privileges assigned to the user by administrator, an end user can view but cannot change most of the parameters associated with Craft procedures. For more information, see the applicable user guides.

Administrative Procedure value (in English)	Purpose	See
8021X	Set 802.1X operational mode	Setting the Operational Mode to 802.1X on page 58
ADDR	Address information programming	Use the pre-installation checklist.
AGC	Enable/disable Automatic Gain Control	Disabling/enabling automatic gain control on page 234
CLEAR	Clear all values to factory defaults	Clearing the deskphone settings on page 61
DEBUG	Enable/disable Debug Mode	Enabling and disabling the debug mode on page 62
GROUP	Set the Group Identifier	Changing the group identifier on page 236
HSEQUAL	Handset audio equalization	Setting handset audio equalization on page 235
INT	Interface Control	Changing Ethernet interface control on page 63
LOG	Enable/disable Event Logging	Disabling/enabling event logging on page 64
LOGOUT	Log off the deskphone	Logging off The deskphone on page 65
MLS	View Multi-Language text Strings	Viewing multi-language strings on page 66
RESET VALUES	Reset system initialization values to defaults	Resetting system values on page 66
RESTART PHONE	Restart the deskphone	Restarting The deskphone on page 67
SIG	Set the signaling protocol download flag	Changing the signaling protocol.
SSON	Set the Site-Specific Option Number	Changing SSON settings on page 68
TEST	Initiate a self-test	Performing a self-test on page 69
VIEW	View current parameter values and file names	Using The VIEW craft procedure for troubleshooting on page 248
VPN	Administer and view Virtual Private Network (VPN) settings	<i>VPN Setup Guide for 9600 Series IP Telephones</i>

*** Note:**

1. If the deskphone software has VPN and media encryption disabled, VPN will not appear on the Craft procedures menu list. To determine if this applies to the deskphone, go to the About Avaya IP Deskphone screen through the Avaya (A) Menu or Home screen as applicable to the phone, and select the Settings list.

Related links

[Local Administration menu procedures](#) on page 52

Setting the operational mode to 802.1X

About this task

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

Procedure

1. When you select 802.1X from the Craft Procedures screen, the deskphone displays the following:

```
Supplicant:  
Pass-thru:
```

where the Supplicant line is the text string associated with the current system value of DOT1XSTAT. The DOT1XSTAT parameter configures the 802.1X Supplicant Mode operation control, defined as:

The options that are displayed depend on the following parameters as set in the `46xxsettings.txt` file:

- *Disabled* if DOT1XSTAT = 0
- *Unicast-only* if DOT1XSTAT = 1
- *Unicast/multicast* if DOT1XSTAT = 2

The Pass-thru line is a text string associated with the current system value of DOT1X where:

- *Enabled mode* if DOT1X = 0
- *Enabled w/Logoff* if DOT1X = 1
- *Disabled* if DOT1X = 2

2. Select the line you want to change.

Depending on which line you selected to change, the phone displays the following text:

```
Current setting:  
New Setting:
```

3. To change the setting, press the Right or Left navigation arrow to navigate through the applicable settings .

Depending on the current value, the deskphone selects the next sequential text string displays it as the New setting. For example when you change the Pass-thru mode, if the current value is Pass-thru mode, pressing the Choice Selector causes the deskphone to display P-t w/Logoff. If the current setting is disabled, pressing the Choice Selector changes the new setting to Pass-thru mode.

4. Press **Save** to store the new setting and redisplay the Craft Procedures screen.

Related links

[Local Administration menu procedures](#) on page 52

Changing IP address information

About this task

Use this procedure to assign a static IP address to the deskphone.

Caution:

Static addressing is necessary when a DHCP server is unavailable. But static addressing has room for text entry errors. So Avaya recommends that you install a DHCP server and do not use static addressing.

Important:

IPv6 operation is limited to a specific customer set and is not for general use.

Use the following procedure to invoke manual address information programming.

Procedure

1. Select ADDR from the Craft Procedures screen. The next screen displays the following fields with the prompt `Select address to change.`

Static addressing field	Field value	Description
Phone (IPv4)	nnn.nnn.nnn.nnn	phone IP address (IPADD)
Phone (IPv6)	hhhh:hhhh::hhhh:hhhh:hhhh	phone IP address (NVIPADDV6)
Call Server	nnn.nnn.nnn.nnn hhhh:hhhh::hhhh:hhhh:hhhh	Call Server in use; media server IP address
Router (IPv4)	nnn.nnn.nnn.nnn	Router in use; gateway/router IP address
Mask (IPv4)	nnn.nnn.nnn.nnn	IP network mask (NETMASK)
HTTP Server	nnn.nnn.nnn.nnn hhhh:hhhh::hhhh:hhhh:hhhh	IP address of HTTP File Server in use
HTTPS Server	nnn.nnn.nnn.nnn hhhh:hhhh::hhhh:hhhh:hhhh	IP address of HTTPS (TLS) File Server in use

Table continues...

Static addressing field	Field value	Description
802.1Q	L2Q text string	L2Q setting text description
VLAN ID	dddd	NVL2QVLAN
VLAN Test	ddd	VLANTEST

where:

- *nnn.nnn.nnn.nnn* is the current IP address in IPv4 format associated with the specific address information on the left side, which could be either a value previously set by a technician, or the original value of NVIPADD if no previous change was made.
 - *hhhh:hhhh:hhhh:hhhh* is the current IP address in IPv6 format associated with the specific address information on the left side, which could be either a value previously set by a technician, or the original value of NVIPADD if no previous change was made.
 - *L2Q text string* is the text string associated with the current system value of L2Q where *Auto* = an L2Q value of 0, *On* = an L2Q value of 1, and *Off* = an L2Q value of 2.
 - *dddd* is the current value of NVL2QVLAN and *ddd* is the current value of VLANTEST, respectively.
2. Use the navigation arrows to scroll to and highlight the address you want to change, then press **Change** to display the change screen for that specific address value.
 3. Select one of the following as appropriate to the item you selected:

Task	Steps
To change any of the IP address values such as Phone, Call Server, Router, Mask, and File Server	<p>Use the dial pad to enter the new IP address. IP addresses have three sets of three digits followed by a period. Pressing star (*) following entry of three digits causes a period to be placed in the next position, and the cursor to advance one position to the right. If you press the star (*) and enter an IPv6 address, a colon is inserted into the input buffer and the cursor is moved to the next character location. The exceptions are entry of a Router or Mask address, which follows the IPv4 method of inserting a period rather than a colon. For example, to enter the IP address 111.222.333.444 in IPv4 format, press the number 1 on the dial pad three times then press *, press the number 2 on the dial pad three times then press *, press the 3 on the dial pad three times then press *, then press the 4 on the dial pad three times.</p> <p>To enter an IP address in IPv6 format, use the dial pad in numeric-only mode entry. For example, pressing button 2 initially enters a 2, followed by A, B, C, and back to 2. Pressing button 3 initially enters a 3, followed by D, E, F, and back to 3.</p> <p>Proceed to the next step.</p>
To change the 802.1Q value	Use the Right navigation arrow to navigate through the text strings corresponding to the L2Q values defined as <i>Auto</i> if L2Q=0, <i>On</i> if L2Q=1, and <i>Off</i> if L2Q= 2 until the text string of the value you want to change to displays. Proceed to the next step.

Table continues...

To change the VLAN ID value	Use the dial pad to enter the new static VLAN ID of from 0 to 4094, inclusive. Proceed to the next step.
To change the VLANTEST value	Use the dial pad to enter the new value of the DHCP OFFER wait period of from 0 to 999. Proceed to the next step.

4. Press **Save** to store the new setting and redisplay the ADDR screen or **Cancel** to return to the ADDR screen without saving the value entered.

Once the new values are stored, the phone resets automatically.

Related links

[Local Administration menu procedures](#) on page 52

Clearing the phone settings

About this task

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

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

- The software load. If you upgrade the phone, the phone retains the latest software. After you clear a phone of the settings, you can administer the phone normally.
- The user configuration stored in backup/restore file server.

Caution:

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

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

Procedure

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

The phone prompts for confirmation.

2. Press one of the following:

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

The phone displays the following text:

```
Clearing values...
```

The phone is reset to the default factory settings.

- All system values and system initialization values.
- 802.1X identity and password.
- User options, parameter settings, identifiers, and password.
- Any user data like Contact Lists or Call Logs are deleted.

After clearing the values, the phone resets.

Related links

[Local Administration menu procedures](#) on page 52

Debug mode

About this task

You can use the debug mode to send all your debug data in a file, `nnn_report.tar.gz` where you replace `nnn` by the deskphone extension as specified by the user during registration.

* Note:


The DEBUG option is available for use only if you change the default password to the craft menu through the PROCPSWD parameter. If you do not change the default password, the option is available only in a read-only mode.

The new value of the PROCPSWD parameter must be 4 to 7 numeric digits, "0000" through "9999999". However if value of PROCPSWD is less than 4 digits after you install Release 6.2.4 or later, the value will be changed back to the default value of 27238.

Procedure

1. Scroll and select DEBUG from the Craft Local Procedure Screen. Press **Start**. The deskphone displays, the following text:

Setting	Options available
Serial Port	Adjunct/CLI/Disable
Log to file	On/Off
Phone Report	Navigate to Phone Report . Press Create to send the report to the backup folder specified by BRURI. <div> <div>* Note:</div> <div>The Phone Report option is available only if backup and restore is enabled.</div> </div>
Port Mirroring	On/Off

Setting	Options available
Profile	H.323 signaling over TLS to On/Off
Service	Service mode control/Service mode record to On/Off
SSH Status	Enabled/Disabled  Note: The SSH Status option displays an Active status if an SSH connection is already established.
SSH Fingerprint	

2. Scroll to the option that you want to change and press **Change** or touch **OK** to toggle the selected setting from the available options. The deskphone displays the softkeys **Save**, **Change**, and **Cancel**.
3. If you have made any changes to the Debug Mode option, then you must press or touch the **Save** option. This action resets the phone and saves the changes to the debug screen.

 **Note:**

When SSH is manually enabled, the SSH port will only be opened for one SSH connection. When that connection is terminated, the port will be closed, and it must be reopened (SSH must be re-enabled) from the Craft Debug procedure if another connection is to be established.

Related links

[Local Administration menu procedures](#) on page 52

Changing Ethernet interface control

About this task

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

Procedure

1. When you select INT from the Craft Procedures screen, the phone displays the following options with a prompt to use the Right and Left navigation arrows to select a setting:

Ethernet	Choice Selector
PC Ethernet	Choice Selector

The options that are displayed are the text strings associated with the current PHY1STAT on the Ethernet line and the current PHY2STAT system value on the PC Ethernet line.

- **Auto** when PHY1STAT = 1
- **10 Mbps half** when PHY1STAT = 2
- **10 Mbps full** when PHY1STAT = 3

- **100 Mbps half** when PHY1STAT = 4
- **100 Mbps full** when PHY1STAT = 5
- **1000 Mbps full** when PHY1STAT = 6

The PHY2STAT text strings are:

- **Disabled** when PHY2STAT = 0
 - **Auto** when PHY2STAT = 1
 - **10 Mbps half** when PHY2STAT = 2
 - **10 Mbps full** when PHY2STAT = 3
 - **100 Mbps half** when PHY2STAT = 4
 - **100 Mbps full** when PHY2STAT = 5
 - **1000 Mbps full** when PHY2STAT = 6
2. To change the Ethernet setting, press the Right navigation arrow to navigate 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) and if you press the Right navigation arrow, the value changes to 10 Mbps full (3). If the current value is 1000 Mbps full (6) and if you press the right navigation arrow, the value changes to Auto (1).
 3. To change the PC Ethernet setting, select that line and press the Right navigation arrow to navigate through the possible settings.
 4. Press **Save** to store the new settings and redisplay the Craft Procedures screen.

Related links

[Local Administration menu procedures](#) on page 52

Disabling and enabling event logging

About this task

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

Procedure

1. When you select *LOG* from the Craft Local Procedure Screen, the deskphone prompts you to use the Right and Left navigation arrows to select a setting and displays the following text:

Log: <i>text string</i>	Choice Selector
-------------------------	-----------------

where the *text string* is the wording associated with the current system value of NVLOGSTAT, defined as:

- **Disabled** when NVLOGSTAT = 0

- **Emergencies** when NVLOGSTAT = 1
 - **Alerts** when NVLOGSTAT = 2
 - **Critical** when NVLOGSTAT = 3
 - **Errors** when NVLOGSTAT = 4
 - **Warnings** when NVLOGSTAT = 5
 - **Notices** when NVLOGSTAT = 6
 - **Information** when NVLOGSTAT = 7
 - **Debug** when NVLOGSTAT = 8
2. To change the setting, press the Right or Left navigation arrow to navigate 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 Alerts (2), pressing the Right navigation arrow changes the value to Critical (3). If the current value is Debug (8), pressing the Right navigation arrow changes the value to Disabled (0).

3. Press **Save** to store the new setting and redisplay the Craft Local Procedure screen.

Related links

[Local Administration menu procedures](#) on page 52

Logging off from the phone

About this task

Use the following procedure to log off from a phone.

Caution:

Once you are logged off from a phone, you might need a password and extension to log back in.

Procedure

1. When you select **LOGOUT** from the Local Craft Procedures screen, the phone displays the following text:

Press Log Out again to confirm.

2. Press or tap **Log Out** to log off from the phone.

Press **Cancel** to return to the Local Craft Procedures screen without logging off the phone.

Related links

[Local Administration menu procedures](#) on page 52

Viewing multilanguage strings

About this task

Use this procedure to view the language strings available on the deskphone. A language string is any set of words or phrases on the IP deskphone user interface in the currently active language.

Procedure

1. Select MLS from the Craft Procedures screen. The deskphone displays the following text:

```
Tag # N
Text string for tag # N      text string
```

where *N* is the label associated with a specific language in the downloaded language file and *text string* is the wording associated with that Tag number.

2. Use the Up and Down navigation arrows to scroll through the list of text strings.
Use the Right and Left navigation arrows to scroll right or left one character at a time to view the entire text string, if it exceeds the available display line space.
3. Press **Back** to return to the Craft Procedures screen.

Related links

[Local Administration menu procedures](#) on page 52

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 **Craft Procedures** screen. The phone displays the following text:
2. Press one of the following:
 - **Reset**: To start the phone reset.
 - **Cancel**: To return to the previous screen.

The phone resets from the beginning of registration, which might take a few minutes. The phone resets:

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

Related links

[Local Administration menu procedures](#) on page 52

Restarting the phone

About this task

Use the following procedure to restart the phone.

Procedure

1. Select **RESTART PHONE** from the Craft Procedures screen. The phone displays the following text:

```
Press Restart to confirm.
```

2. Press **Cancel** to return to the Craft Procedures screen without restarting the phone.

Press **Restart** to proceed with the registration steps.

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

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

Related links

[Local Administration menu procedures](#) on page 52

Setting or changing the signaling protocol

About this task

Use the following procedure to set or change the Signaling Protocol Identifier. 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. Select SIG from the Craft Local Procedures screen. The deskphone prompts you to use the Right and Left navigation arrows to select a setting and displays the following text:

```
Sig: 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

2. Press the Right or Left navigation arrow to navigate through the settings to change the setting.

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 the Right arrow changes the value to 2 (SIP).

3. Press **Save** to store the new setting and redisplay the Craft Procedures screen.

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

Related links

[Local Administration menu procedures](#) on page 52

Changing SSON settings

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). SSON default value is 242.

Procedure

1. Select SSON from the Craft Procedures screen.

The phone displays the following text:

```
Current setting:  
New Setting:
```

where the *setting* is the current system value of NVSSON.

2. To change the setting, use the dial pad to enter a valid SSON value between 128 and 255.
3. Press **Save** to store the new setting and redisplay the Craft Procedures screen.

Related links

[Local Administration menu procedures](#) on page 52

Performing a self-test

About this task

Note:

IP deskphone stores two software code images in reprogrammable non-volatile memory. The primary image, called the “big app” must be running to perform a self-test. The backup image, called the “little app” does not support the self-test.

Use the following procedure to perform self-testing:

Procedure

1. Tap or select **TEST** from the Craft Procedures screen. The phone displays the following text:

Press Test to confirm.

2. Tap or press **Test** to start phone testing.

Tap or press **Cancel** to return to the Craft Procedures screen without testing the phone.

The test performs the following actions:

- Removes labels on all softkeys.
- Illuminates groups of LEDs at a time on the phone and any attached button modules sequentially for about a half second. Illumination starts with the upper half of the phone and continues through the lower half of any attached button module in a repeating cycle.
- Shows pixels on the display with highest intensity.

After approximately 5 seconds, the top phone screen displays either *Self-test passed* or *Self-test failed*.

3. Press or tap **Back** to return to the Craft Procedures screen.

Related links

[Local Administration menu procedures](#) on page 52

Post installation checklist for 9600 and J100 IP Phones

To ensure that the J100 phone is properly installed and running properly, verify that the following requirements are complete.

No.	Task	Reference	✓
1	Has the phone acquired an IP address?	N/A	
2	Are you able to make a call from the phone?	For more information, see device specific using guide.	
3	Are you able to modify the 46xxsettings.txt file parameters and end user settings.	Accessing the Administration menu after phone startup on page 54	
4	Are you able to upgrade your phone?	Upgrading the device on page 222	
5	For security considerations, have you configured the phone setup with TLS signaling? Have you installed the appropriate private network authentication certificates?		

To ensure that the 9600 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 <i>Using Avaya 9608/9608G/9611G IP Deskphones SIP, Using Avaya 9621G/9641G/9641GS IP Deskphones H.323</i> .	
Are you able to perform backup-restore?		
Are you able to change deskphone settings?	See <i>Accessing Craft procedures during normal operation</i> .	
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 <i>Administering Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323</i> .	

Chapter 4: Administering your phone

Administrator responsibilities

To administer the phone, complete the tasks in the order shown.

1. Administer the switch.
2. Administer LAN and applicable servers to accept the deskphones.
3. Download the deskphone software from the Avaya support site.
4. Update the `46xxsettings.txt` file with site-specific information, as applicable.
5. Install the phone.
6. Update phone using Craft procedures, as applicable.

Logging in to your phone as an administrator

About this task

Perform this task to log in to your phone. Log in from the initial screen when it prompts you for your extension.

The phone stops at the discovery mode in the following conditions:

- The login credentials are incorrect.
- The phone is logged in but one of the gatekeepers is not reachable because of an upgrade or a network outage. In the discovery mode, press **Reset**. The phone deletes the credentials from the memory, reboots, and displays the Login page.

If the administrator has enabled the offline Call Log feature on the deskphone, the deskphone downloads the call log database when you log in. The offline call log database stores the calls that landed on the deskphone while you were not logged in. These calls are added to the call history as missed calls.

Procedure

1. Press **Login**.
2. Enter your extension.
3. Press **Enter** or **OK** or **#**.

4. Enter your password. Enter the password that the administrator assigned to you.
5. If your administrator configured the system to allow visiting users, the deskphone prompts for the Login mode. Use the right or left navigation arrow to indicate whether you are a visiting user of this deskphone (**Visiting User**) or not (**Default**).
6. Press **Enter** or **OK** or **#**.

Initial administration checklist

System and LAN administrators must use the following checklist to ensure that all phone system prerequisites and phone requirements are met prior to phone installation:

Table 4: Initial Administration Checklist

#	Task	Description	Related information	✓
1	Install the hardware.	Check whether the network hardware can handle the phone system requirements.	Network Requirements on page 85.	
2	Install the license for call server.	-	Communication Manager Administration on page 98.	
3	Configure the VoIP settings.	-	-	
4	Configure the settings on each phone.	-	-	
5	Install the DHCP server.	Set up DHCP-specific parameters.	Vendor-provided instructions.	
6	Install the HTTP/HTTPS server.	When installing HTTP/HTTPS, ensure that it is installed on at least one new or existing computer that is connected to the LAN.	Vendor-provided instructions.	
7	Download the following files: <ul style="list-style-type: none"> • Application files • Script file • 46xxsettings.txt file 	Download the files from the Avaya support site.	www.avaya.com/support Telephone Software and Application Files on page 122.	

Table continues...

#	Task	Description	Related information	✓
8	Edit the 46xxsettings.txt file.	Use your own tools to edit the 46xxsettings.txt file as required.	Telephone Software and Application Files on page 122.	
9	Add WML servers.	You can add WML content as applicable to new or existing WML servers. Administer the content that the WML push servers push on to the deskphones as applicable.	<i>Avaya IP Deskphone Edition for 9600 IP Telephones Application Programmer Interface (API) Guide</i>	
10	Local administration of deskphones if applicable.	As a Group:	Using the GROUP parameter to set up customized groups on page 125	
		Individually:	The applicable Craft Local Procedures.	
11	Phones installation in the network.	-		
12	User modification of Options, if applicable.	-	OPSTAT and the respective User Guide for the specific deskphone model.	
13	VPN functionality administration, if applicable.	Enable or disable VPN, provide administration for your particular VPN environment.	<i>VPN Setup Guide for 9600 Series IP Telephones</i>	

Administrative requirements

The following operating environment for the phone are:

- Phone Administration on the Avaya call server.
- IP address management for the phone.
- Tagging Control and VLAN administration for the phone, if applicable.
- Quality of Service (QoS) administration for the phone, if appropriate.
- Protocol administration, for example, Simple Network Management Control (SNMP) and Link Layer Discovery Protocol (LLDP).
- Interface administration for the phone, as appropriate. Administer the phone to LAN interface using the PHY1 parameter.

Administer the deskphone to computer interface using the PHY2 parameter.

- Application-specific phone administration, if applicable.

Related links

[Parameter data precedence](#) on page 74

[Initialization process overview](#) on page 74

[JITC security compliance mode overview](#) on page 79

[Error conditions](#) on page 85

Parameter data precedence

If you administer a parameter in multiple places, the last server to provide the parameter takes precedence. The following is a list of precedence, from lowest to highest:

1. Manual administration. Call server or HTTP server or both are two exceptions for the phone parameter STATIC.
2. DHCP, except as indicated in “DHCPACK Setting of Parameter Values” in [Setting up the DHCP server](#) on page 109.
3. The `46xxsettings.txt` file.
4. The Avaya call server.
5. Backup files, if administered and permitted.
6. LLDP: Only the IPv4 mode supports LLDP.

Note:

Setting the call server and file server IP addresses have the lowest precedence.

Related links

[Administrative requirements](#) on page 73

Initialization process overview

The deskphone initialization process includes exchange of information that happens when the phone initializes and registers. The process includes the following five steps.

You must administer all equipment properly prior to initialization.

Note:

When you start a deskphone without access to the HTTP server, the phone reuses parameters from before the reboot. The phone waits for 60 seconds and starts with the old parameters.

Related links

[Administrative requirements](#) on page 73

[Connection to network](#) on page 75
[DHCP processing](#) on page 75
[File downloads](#) on page 75
[Certificates usage](#) on page 76
[Registration with the call server](#) on page 77
[Connection to network](#) on page 75
[DHCP processing](#) on page 75
[File downloads](#) on page 75
[Certificates usage](#) on page 76
[Registration with the call server](#) on page 77

Connection to network

The phone is appropriately installed and powered. After a short initialization process, the phone displays the speed at which it is connected to the network and determines whether to initiate 802.1X network access procedures.

Related links

[Initialization process overview](#) on page 74
[Initialization process overview](#) on page 74

DHCP processing

If an IP address has not been manually configured in the phone, the phone initiates DHCP. Among other data passed to the phone is the IP address of the HTTP or HTTPS server.

Related links

[Initialization process overview](#) on page 74
[Initialization process overview](#) on page 74

File downloads

Avaya phone uses the HTTP server to download software. The HTTPS server is used to download upgrade file, configuration files, language files, certificate files and to backup or restore user information.

The phone first downloads the upgrade file to identify the latest software files. Then, the phone downloads the settings file to identify the required language files and/or certificate files. Finally, the phone downloads software files depending on the software of the phone and if it is the same as that specified in the upgrade file.

Note:

HTTPS can be used to download configuration files only. Software files are downloaded using HTTP only (no HTTPS file download is supported). Configuration files can be downloaded using HTTP or HTTPS.

Related links

[Initialization process overview](#) on page 74

[Initialization process overview](#) on page 74

Certificates usage

The H.323-based phones use certificates to verify the authenticity of the following:

- HTTPS file server for downloaded configuration files, and user backup and restore files.
- H.323 signaling over TLS.
- VPN, when certificate authentication method is used.
- SLAMon server.
- SSO applications.
- 802.1x EAP-TLS.

Related links

[Initialization process overview](#) on page 74

[Certificate revocation](#) on page 76

[Initialization process overview](#) on page 74

[Certificate revocation](#) on page 76

Certificate revocation

The certificates are published by the certificate authority with information about the revocation status. The deskphones use Online Certificate Status Protocol (OCSP) to verify the revocation status of all the certificates in the chain between the server certificate and the root certificate. The root certificate is not verified. The revocation check of the certificates is done by sending HTTP or HTTPS requests to the OCSP server.

The certificates may or may not include the authority information access (AIA) extension.

The OCSP responder follows RFC 2560. The deskphones accept only signed responses. The validation of the signed response is done by using one of the three options mentioned in section 4.2.2.2 in the RFC:

1. The OCSP response is signed using CA which is trusted certificate is administered using OCSP_TRUSTCERTS.
2. The OCSP response is signed using CA which is also used to sign the certificate in question.
3. The OCSP response is signed using CA which includes a value of id-kp-OCSPSigning in an ExtendedKeyUsage extension and is issued by the CA that issued the certificate in question.

The following `46xxsettings.txt` file parameters are used by OCSP for certificate revocation:

- OCSP_ENABLED
- OCSP_URI
- OCSP_URI_PREF

- OCSP_ACCEPT_UNK
- OCSP_NONCE
- SERVER_CERT_RECHECK_HOURS
- OCSP_TRUSTCERTS

Related links

[Certificates usage](#) on page 76

[Certificates usage](#) on page 76

Registration with the call server

The call server referred to in this section is Avaya Aura[®] Communication Manager.

The phone is registered with the call server in two modes, named registration and unnamed registration.

Named registration

In this step, the phone might prompt the user for an extension and password. The phone uses that information to exchange a series of messages with the call server. For a new installation and for full service, the user can enter the phone extension and the password configured on the call server for that particular extension. The information required to restart a phone that was previously registered with an extension number is already stored on the phone. The user must confirm the information so that the phone is appropriately registered and can download call server data such as feature button assignments.

Unnamed registration

Unnamed registration provides the telephone with a restricted class of service, such as emergency calls, if administered on the call server. Using this feature, you can register a deskphone with the call server without an extension. To invoke Unnamed Registration, either enter a null (empty) extension or password or take no action. Unnamed registration is controlled on both the Communication Manager and the UNNAMEDSTAT parameter in the `46xxsettings.txt` file.

The UNNAMEDSTAT specifies whether unnamed registration is initiated by the deskphone, if a value is not entered at the extension registration prompt within 60 seconds. Valid values for this parameter are:

- 0: Disabled
- 1: Enabled

You can choose to take no action and allow the “Extension...” prompt to display for 60 seconds. The phone automatically attempts to register by means of Unnamed Registration.

A phone registered with Unnamed Registration has the following characteristics:

- Only one call appearance
- No administrable features
- Outgoing calls only, subject to call server Class of Restriction or Class of Service limitations
- Conversion to normal named registration possible by the user entering a valid extension and password.

Related links

[Initialization process overview](#) on page 74

[Other administrable options using parameters](#) on page 78

[Initialization process overview](#) on page 74

[Other administrable options using parameters](#) on page 78

Other administrable options using parameters

- MCIPADD

You can configure the phone to register to a particular call server by listing the IP addresses in the MCIPADD parameter in DHCP or the `46xxsettings.txt` file. The standard practice is to list the CLANs on the main call server, followed by any Enterprise Survivable Server (ESS) addresses, followed by any Local Spare Processor (LSP). To deviate from this practice, you can list CLANs for multiple main call servers. In general, the phone will start from the beginning of MCIPADD and attempt to register with each IP address in turn, one at a time, until the phone gets a positive response. If MCIPADD is administered, users can register to local call servers.

- VUMCIPADD

Visiting User (VU) registration is when a user from another location wants to register with their home call server using their home extension. The phone support VU registration by using the VUMCIPADD parameter.

When this parameter contains one or more IP addresses, the user sees a slight change to the Login screen. In that screen the user is asked to specify a Login Mode of either Default or Visiting User. If the user selects Default, the deskphone uses the MCIPADD parameter value whereas if the user selects Visiting User, the deskphone attempts to register with each IP address in VUMCIPADD simultaneously until it gets a positive response.

 **Note:**

Only the Challenge and Annex-H profiles are supported in the VU mode.

For example, if the company has locations in cities A, B, C, and D, you can administer VUMCIPADD with one IP address from each of the main call servers in the four cities. A user from city A is in the city B location but wants to use the city A call server. The user selects Visiting User on the Login screen, the deskphone contacts each of the four main call servers simultaneously and registers with the only call server that gives a positive response for city A.

- UNNAMEDSTAT

Specifies whether unnamed registration is initiated by the deskphone, if a value is not entered at the extension registration prompt within 60 seconds. Valid values for this parameter are:

- 0: Disabled
- 1: Enabled

Related links

[Registration with the call server](#) on page 77

[Registration with the call server](#) on page 77

JITC security compliance mode overview

The Avaya phone H.323 firmware Release 6.8 adheres to the Joint Interoperability Test Command (JITC) security compliance requirements. According to the US Department of Defense guidelines summarized in the UCR document, these security features must be supported by the setup. These features were tested by JITC.

Avaya Aura® Communication Manager 6.3.6 and later support the JITC security compliance mode. In the JITC security compliance mode, Communication Manager and the deskphones communicate using the certified algorithms of Federal Information Processing Standards 140-2.

Supported features

The following features are supported in the JITC security compliance mode:

- Random number generator PRNG [SP 800-90] DRBG using CTR DRBG (AES-256), with deviation function enabled
- H.323 signaling over TLS or Annex-H
- SRTP using 1-sertp-aescm128-hmac80 cipher suite
- Image, settings files, or certificates download over HTTP or HTTPS
- Backup and restore configuration files
- PKCS12 file generated in FIPS mode
- OCSP
- LLDP
- SNMPv2c
- Syslog
- Call center environment including Agent Greeting files

The following features are not supported in the JITC security compliance mode:

- SSH server
- IPsec VPN tunnels
- Visiting users
- SLA Monitor
- Push server
- WML browser
- SSO
- 802.1x EAP-TLS
- SCEP

*** Note:**

H.323 signaling over TLS is supported in both FIPS and non-FIPS mode.

Related links

[Administrative requirements](#) on page 73

[JITC security compliance mode configuration](#) on page 80

[JITC security compliance mode configuration](#) on page 80

JITC security compliance mode configuration

You must configure the deskphone to work in the security mode in which the UCR requirements to the JITC test cases are complied. In the `46xxsettings.txt` file, set the parameters to the values specified in the table below.

Parameter	Value	Description
FIPS_ENABLED	1	Use cryptographic algorithms using embedded FIPS 140-2-validated cryptographic module.
PROCSTAT	0	Enables local CRAFT procedure.
PROCPSWD	Obtained from Communication Manager, DHCP server, or file server	<p>Restricts the use of the default administration password of the deskphone. The value can be set on Communication Manager, DHCP server, or file server.</p> <p>* Note:</p> <p>Obtaining PROCPSWD through Communication Manager is the most secure method. Setting PROCPSWD using HTTPS is secure only if mutual certificate authentication is done.</p>
PKCS12URL	URL of the PKCS #12 file	The PKCS #12 file contains an identity certificate for the deskphone, and the corresponding private key. After the file is downloaded by the phone, the user is required to enter the password.
TRUSTCERTS	List of trusted certificate files	Trust certificates are used as trust points for TLS connections.

Table continues...


Parameter	Value	Description
TLSSRVRVERIFYID	1	To verify the identity of the TLS server against the identity in the certificate. The identity of server as presented in subject common name or subjectAltName is compared with the relevant IP address or host name of the server. The server is configured using BRURI for Backup/restore over HTTPS, TLSSRVR for HTTPS file server for configuration files download, and MCIPADD for H.323 over TLS signaling.
OCSP_ACCEPT_UNK	1	Specifies whether a certificate is authenticated even if its revocation status cannot be determined. Valid values are: 0 to 1.
OCSP_ENABLED	1	<p>Specifies whether OCSP is used to verify the revocation status of the certificates.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • 0: OCSP is not used. • 1: OCSP is used to check the revocation status for the certificates presented by peers for any TLS connection. For example, HTTPS, 802.1x with EAP-TLS, SLA Mon agent, IPsec VPN, or SSO. <p> Note:</p> <p>H.323 over TLS, Backup/restore, and file downloads are the only applications supported in the secured mode. 802.1x EAP-TLS, SLA Mon, IPsec, VPN, and SSO are not supported.</p>

Table continues...

Parameter	Value	Description
OCSP_URI_PREF	1	<p>OCSP responder URI can either be obtained from the certificate presented by the server, or can be locally configured on the phone in OCSP_URI.</p> <p>OCSP_URI_PREF specifies the preference between the two sources.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • 1: OCSP_URI_PREF is used first and then the value from the OCSP field of the Authority Information Access (AIA) extension of the certificate is checked. • 2: OCSP field of the Authority Information Access (AIA) extension of the certificate is checked first and then OCSP_URI_PREF is used.
OCSP_URI	URI of the OCSP responder	Specifies a URI for an OCSP responder. The URI can be an IP address or a host name.
OCSP_NONCE	1	<p>Specifies whether a nonce is included in OCSP requests and expected in OCSP responses.</p> <p>Valid values are: 0 or 1.</p>
OCSP_TRUSTCERTS	List of the trusted OCSP certificate files	<p>Specifies the list of the trusted OCSP certificates to be downloaded. Acts as a separate trusted certificate repository for the OCSP Trusted Responder Model and contains certificates to be trusted by the OCSP responder.</p> <p>Local OCSP trusted certificates are used for cases where the OCSP responder certificate is signed by a CA that is different from the one used to sign the server certificate.</p>

Table continues...


Parameter	Value	Description
TLS_SECURE_RENEG	1	Specifies whether a TLS session should be terminated if the peer does not support secure renegotiation. Valid values are 0 or 1.
HTTPSRVR	IP address of the HTTP server	Used to download only the firmware files by HTTP.
TLSSRVR	IP address of the HTTPS server	Used to download the configuration files by using HTTPS.
AUTH	1	Used to enforce download of configuration files using HTTPS only. <div>  Note: If AUTH is set to 1, and the trusted certificate repository is not null, the phone will only download configuration files from HTTPS that has a certificate signed by CA. The root certificate of this CA must be in the trusted certificate repository. </div>
OPSTAT	101	Restricts displaying the configuration information on the deskphone.
SNMPSTRING	Null	Avaya J169/J179 IP Phone supports SNMPv3
SSH_ALLOWED	0	Disables SSH.
NVVPNMODE	0	VPN not supported in the FIPS mode.
VPNPROC	0	VPN not supported in the FIPS mode.
TPSLIST	Null	Push server does not support TLS.
VLANSEP	1	Enables VLAN separation that restricts the computer connected to the PC port from connecting to the phone VLAN.

Table continues...

Parameter	Value	Description
VLANSEPMODE	1	Enforces VLAN separation. When set to 1, VLAN separation is enforced for both untagged and tagged packets from the computer and the network port. The computer cannot send tagged or untagged packets to the deskphone processor.
L2QVLAN	Address of the voice VLAN	The deskphone sends the untagged data packets to this VLAN. The value must not be 0 or the PHY2VLAN address.
L2Q	0: Auto 1: On	0: Auto - The deskphone starts sending tagged packets to the voice VLAN. If the VLANTEST timer has expired, the phone sends untagged packets. 1: Tagging – The deskphone starts sending tagged packets on voice VLAN and if VLANTEST timer expires, the phone then sends tagged packets on VLAN==0.
PHY2VLAN	Address of the data VLAN	The deskphone sends the tagged data packets to this VLAN. The value must not be 0 or the L2QVLAN address.
CERT_WARNING_DAYS	60	Applies to trusted certificates, OCSP certificates, and identity certificate. Specifies the number of days before the expiration of a certificate that a warning should first appear on the phone screen. Log and syslog messages are generated for expired certificates. Valid values are 0 to 99. The value 0 disables the warning.
Console port	Disabled	Restricts the access to the console port. The serial port under CRAFT > DEBUG must be set to Adjunct.
WMLIDLEURI	Null	Disables the WML browser on the deskphone.

Table continues...

Parameter	Value	Description
WMLHOME	Null	Disables the WML browser on the deskphone.
AUTOANSSTAT	0	Disables auto-answer.
GUESTLOGINSTAT	0	Disables the guest login feature.
VUMCIPADD	Null	Disables the visiting user login.

Related links

[JITC security compliance mode overview](#) on page 79

[JITC security compliance mode overview](#) on page 79

Error conditions

Assuming proper administration, most of the problems reported by phone users are likely to be LAN-based or Quality of Service. Server administration and other issues can impact user perception of IP phone performance.

Related links

[Administrative requirements](#) on page 73

Network requirements

Network assesment

Perform a network assessment to ensure that the network has the capacity for the expected data traffic and voice traffic, and can support jitter buffers and the following types of applications as required:

- H.323
- DHCP
- HTTP/HTTPS
- LLDP
- RADIUS

You also need QoS support to run VoIP on your configuration.

To use the IP deskphones to reach the network through a Virtual Private Network 15 (VPN), see *VPN Setup Guide for 9600 Series IP Telephones*.

Hardware requirements

- Category 5e cables that conform to the IEEE 802.3af-2003 standards, for LAN powering.
- TN2602 or TN2302 IP Media Processor circuit pack. For increased capacity, install a TN2602 circuit pack even if you have a TN2302 IP Media Processor circuit pack.
- Avaya Aura 7.0 and later is supported in virtualized environment.
- TN799C or D Control-LAN (C-LAN) circuit pack.

 **Important:**

IP telephone firmware Release 1.0 or later requires TN799C V3 or greater C-LAN circuit packs. For more information, see the *Communication Manager Software and Firmware Compatibility Matrix* on the Avaya support site <https://support.avaya.com/CompatibilityMatrix/Index.aspx>.

Ensure that you administer the appropriate circuit packs on your server.

Server requirements

You can configure three types of servers:

- DHCP server: Avaya recommends that you install a DHCP server and do not use static addressing. Install the DHCP server
- HTTP or HTTPS server: Administer the HTTP or HTTPS file server.
- Web and Push servers (optional): If users have access to corporate WML web sites, administer the deskphones. For push functionality, you need a Trusted Push Server. The Trusted Push Server can be the same server as your WML server. Avaya recommends that you restrict access to folders on the WML server that contain push content.

 **Note:**

The system supports Push only in IPv4 mode. Your Web and push server configuration must be compatible with the requirements mentioned in the *Avaya IP Deskphone Edition for 9600 IP Telephones Application Programmer Interface (API) Guide*.

While the servers listed provide different functions that relate to the phone, the servers are not necessarily different boxes. For example, DHCP provides file management whereas HTTP provides application management, yet both functions can coexist on one hardware unit. Use any standards-based server.

For parameters related to Avaya Server information, see [Communication Manager Administration](#) on page 98, and the administration documentation for your call server. For parameters related to DHCP and file servers, see [Server Administration](#) on page 107.

 **Caution:**

The deskphones obtain important information from the script files on the file server and depend on the application file for software upgrades. If the file server is unavailable when the deskphones reset, the deskphones operate based on the default administration and continue

with the call server registration process. Not all features are available. To restore the features, you must reset the deskphones when the file server is available.

Required network information

Before you administer DHCP, HTTP, and the HTTPS servers, collect the following network information. If you have more than one gateway (router), HTTP/HTTPS server, or call server in your configuration, complete the required network information for each DHCP server before you install the phones.

The phone support specifying a list of IP addresses for a gateway/router, HTTP or HTTPS server, and Avaya call servers. Each list can contain up to 255 total ASCII characters, with IP addresses separated by commas with no intervening spaces. Depending on the specific DHCP server, the phone might support only 127 characters.

When you specify IP addresses for the file server or call server, use either dotted decimal format (xxx.xxx.xxx.xxx) or DNS names for IPv4 addresses. If you use DNS, the value of the DOMAIN parameter is appended to the DNS names that you specify. If DOMAIN is null, you must use DNS names that are fully qualified.

Required network information before installation for each DHCP server

- Gateway router IP addresses
- If the HTTP or the HTTPS file server IP addresses, port number, are different from the default, and the directory path if files are not located in the root directory
- Subnetwork mask
- Avaya call server IP address or addresses
- Phone IP address range
- DNS server address or addresses if applicable

As the LAN or System Administrator, you must also:

- Administer the DHCP server.
- Edit the configuration file on the applicable HTTP or HTTPS file server.

Other network considerations

SNMP enablement

The phone support SNMPv2c and Structure of Management Information Version 2 (SMIv2). The phones also respond correctly to queries from entities that comply with earlier versions of SNMP, such as SNMPv1. The phones respond to queries directed either at the MIB-II or the read-only Custom MIB. Read-only means that you cannot change the values externally with network management tools. H.323 Release 6.4 onwards, SNMP can be used to query the hardware revisions on the phone.

You can restrict the IP addresses from which the phones accept SNMP queries using the SNMPADD parameter. You can also customize your community string with the SNMPSTRING parameter.

Configuration of SNMPSTRING and SNMPADD can also be done using the Communication Manager. The deskphones get this configuration after they register with the Communication Manager.

 **Note:**

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

For more information about SNMP and MIBs, see the IETF website. The Avaya Custom MIB for the deskphones is a part of the software distribution file available for download on the Avaya support site at <http://www.avaya.com/support>.

Ping and traceroute

All phones respond to a ping or traceroute message sent from the call server switch or any other network source. The call server can also instruct the phone to originate a ping or a traceroute to a specified IP address. The phone carries out that instruction and sends a message to the call server indicating the results. For more information about administering an IP telephone system on Communication Manager.

IP address and settings reuse

After you successfully register the phone with a call server, the phone saves the IP address and the parameter values in the non-volatile memory of the phone. The phone can reuse the saved parameters if the DHCP or HTTP/HTTPS server is not available for any reason after a restart. The setting for the DHCPSTD parameter indicates whether to keep the IP address if no response is received for lease renewal. If set to 1 (No) the phone strictly follows the DHCP standard with respect to giving up IP addresses when the DHCP lease expires. If set to 0 (Yes) the phone continues using the IP address until it detects reset or a conflict.

Quality of Service (QoS)

For more information about the extent to which your network can support any or all the QoS initiatives, see your LAN equipment documentation.

IEEE 802.1D and 802.1Q

Three bits of the 802.1Q tag are reserved for identifying packet priority to set any one of the following eight priorities to a specific packet.

- 7: Network management traffic
- 6: Voice for traffic with less than 10 ms latency and jitter
- 5: Video traffic with less than 100 ms latency and jitter
- 4: Controlled-load traffic for critical data applications

- 3: Traffic meriting extra-effort by the network for prompt delivery, for example, executive email
- 2: Reserved for future use
- 0: The default priority for traffic meriting the best-effort for prompt delivery of the network
- 1: Background traffic such as bulk data transfers and backups

 **Note:**

Priority 0 is a higher priority than Priority 1.

Network audio quality

You can monitor network audio performance on the phone while on a call. You can view this information on the Network Information screen. You can view the Network Information screen in Main menu, and select the **Network Information** option directly if available. You can also select **Phone Settings**, then select the **Network Information** option.

While on a call, you can view the network audio quality parameters in real-time. See the following table for the various parameters that you can view:

Table 5: Parameters in real-time

Parameter	Possible values
Received Audio Coding	G.711, G.722, G.726, or G.729.
Packet Loss	No call. The system counts late and out-of-sequence packets as lost if the packets are discarded. The system does not count the packets as lost until a subsequent packet is received and the loss confirmed by the RTP sequence number.
Packetization Delay	No data or an integer number of milliseconds. The number reflects the amount of delay in received audio packets, and includes any potential delay associated with the codec.
One-way Network Delay	No data or an integer number of milliseconds. The number is half the value RTCP or SRTCP computes for the round-trip delay.
Network Jitter Compensation Delay	No data or an integer number of milliseconds reporting the average delay that is introduced by the jitter buffer of the phone.
Internal microphone	The system specifies whether internal microphone is on or off.
Internal speaker	The system specifies whether internal speaker is on or off.

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

IP address list and station number portability

You can specify IP address lists on the phone. On startup or on restart, the phone attempts to establish communication with these various network elements in turn. The phone starts with the first address on the respective list. If the call server denies communication with the phone or the session times out, the phone continues to the next address on the appropriate list and tries that IP

address. The phone does not report failure unless all addresses on a specified list fail, improving the reliability of IP telephony.

The address list and station portability capability also make station number portability possible. Assume a situation where the company has multiple locations in London and New York, that share a corporate IP network. Users want to take the phones from the London office to New York office. When the user starts the phones in the new location, the local DHCP server usually routes the user to the local call server. The local DHCP server if configured correctly, registers the user with call server IP address in London.

TCP/UDP Port utilization

The phone use many protocols, particularly TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and TLS (Transport Layer Security) to communicate with other equipment in the network. Part of this communication identifies which TCP or UDP port each piece of equipment uses to support each protocol and each task within the protocol.

Depending on your network, you must know what ports or ranges to use in the phone operation. Knowing these ports or ranges helps you administer your networking infrastructure. For additional information, see the [Avaya port matrix](#) and the [Avaya website](#).

* Note:

Often, the phones use ports defined by IETF or other standards bodies.

Table 6: Received packets (Destination = IP phones)

Destination port	Source port	Use	UDP or TCP?
The number used in the Source Port field of Qtest packets sent by the phone	7	Received Qtest messages	UDP
22	Any	Packets received by the SSH server of the phone	TCP
The number used in the Source Port field of DNS packets sent by the phone	Any	Received DNS messages	UDP
The number used in the Source Port field of the packets sent by the HTTP client on the phone	Any	Packets received by the HTTP client on the phone	TCP
PUSHPORT	Any	Packets received by the HTTP server of the phone	TCP
500, 2070, or 4500	500 or 4500	Received IKE or IPsec messages (if NVIKEOVERTCP is 1 or 2)	TCP
The number used in the Source Port field of received SSO packet 18414	Any	Received SSO commands	TCP only

Table continues...

Destination port	Source port	Use	UDP or TCP?
546	Any	Received DHCPv6 messages	UDP
The number used in the Source Port field of the TLS/SSL packets that are sent by the HTTP client on the phone	Any	TLS/SSL packets that the HTTP client receives on the phone	TCP
68	Any	Received DHCP messages	UDP
161	Any	Received SNMP messages	UDP
500	Any	Received DHCPv6 messages	UDP
1024 – 5000 (ephemeral port selected by O/S)	Any	Received Traceroute, HTTPS, HTTP messages	Traceroute over UDP HTTP/HTTPS over TCP
1720	Any	Received H.323 signaling messages	TCP
49,300 – 49,309	Any	Received RAS messages	UDP
2048 – 3029	Any	Received RTP, RTCP, SRTP, and SRTCP messages	UDP
500, 2070, or 4500	500 or 4500	Received IKE or IPsec messages (if NVIKEOVERTCP is 0 or 1)	UDP
The number used in the Source Port field of RAS packets that are sent by the phone	1719	H.323 RAS messages	UDP
The next higher port number if the port used for RTP is even, or the next lower port number if the port used for RTP is odd	Any	Received RTCP and SRTCP packets	UDP
The number used in the Source Port field of registration messages that are sent by the SLA agent on the phone	Any	Received SLA registration messages	TCP
Any	1300	H.323 signaling messages in TLS_TTS mode re-registration. Port 1300 is closed when using non TTS method to connect to the gatekeeper or when H.323 signaling is not over TLS. When the port is open, the phone does not respond to incoming packets to this port from IP addresses that are not in the gatekeeper list.	TCP

*** Note:**

CNA is not supported in Release 6.2 and later. SLA is supported in Release 6.4 and later.

Table 7: Transmitted packets (Source = IP phones)

Destination Port	Source Port	Use	UDP or TCP?
7	Any unused port number	Transmitted Qtest messages	UDP
The number used in the Source Port field of packets that are received by the SSH server of the phone.	22	Packets that are transmitted by the SSH server of the phone	TCP
53	Any unused port number	Transmitted DNS messages	UDP
67	68	Transmitted DHCP messages	UDP
HTTPPORT	Any unused port number	Packets that the HTTP client transmits on the phone during startup. Note that when the file server is on Communication Manager, set this value to 81 which is the port required for HTTP downloads rather than the using the default.	TCP
80 unless explicitly specified otherwise, for example, in a URL or because of use of WMLPORT	Any unused port number	Packets that the HTTP client of the phone transmits after startup, for example, for backup and restore or push	TCP
The number used in the Source Port field of the SNMP query packet that the phone receives	161	Transmitted SNMP messages	UDP
The number used in the Source Port field of packets that are received by the HTTP server of the phone	PUSHPORT	Packets that the HTTP server of the phone transmits	TCP
TLSPPORT	411	TCP port number used for HTTPS file downloading. Valid values are 80 through 65535. Note that when the file server is on Communication Manager, set this value to 411 which is the port required for HTTPS downloads rather than the using the default.	TCP

Table continues...

Destination Port	Source Port	Use	UDP or TCP?
411 unless explicitly specified otherwise, for example in a URL	Any unused port number	TLS/SSL packets that the HTTP client of the phone transmits after startup, for example for backup or restore	TCP
500 or 4500	500, 2070, or 4500	Transmitted IKE or IPsec messages, if NVIKEOVERTCP is 0 or 1	TCP
514	Any unused port number	Transmitted Syslog messages	UDP
547	Any unused port number	Transmitted DHCPv6 messages	UDP
1300	Any	H.323 signaling over TLS	TCP
18414	Any unused port number	Transmitted SSO status indications	TCP
33434 - 33523, starts with 33434, increments by 1 for each message sent, 3 messages per hop, up to 30 hops	Any unused port number	Transmitted traceroute messages	UDP
1719	Any unused port number in the range from 49300 to 49309	Transmitted H.323 RAS messages	UDP
2048 – 3029		Transmitted RTP, RTCP, SRTP, and SRTCP messages	UDP
The port number received in the Transport Address field in the RCF message	1720	H.323 signaling messages	TCP
A port number specified in the SLA test request message	SLMPORT	Transmitted SLA test results messages	UDP
A port number specified in the SLA test request message	50012	Transmitted SLA RTP test packets	UDP
33434 – 33523, starts with 33434, increments by 1 for each message sent, 3 messages for each hop, up to 30 hops	50013	Transmitted SLA traceroute messages	UDP
As specified by CM, or as specified in a CNA RTP test request	As specified by CM or as reserved for CNA RTP tests	Transmitted RTP and SRTP packets	UDP

Table continues...

Destination Port	Source Port	Use	UDP or TCP?
The next higher port number if the port used for RTP is even, or the next lower port number if the port used for RTP is odd	The next higher port number if the port used for RTP is even, or the next lower port number if the port used for RTP is odd	RTCP and SRTCP packets transmitted to the far end of the audio connection	UDP
RTCPMONPORT	The next higher port number if the port used for RTP is even, or the next lower port number if the port used for RTP is odd	RTCP packets transmitted to an RTCP monitor	UDP
1719	An unused port number in the range from 49300 to 49309	H.323 RAS messages	UDP
A port number specified in the SLA discovery message	Any unused port number	Transmitted SLA registration messages	TCP
Determined by SNMP mgmt app	161	Transmitted SNMP messages	UDP
Determined by the SSH client or the client Operating system	22	Transmitted SSH messages	TCP

Security

For information about toll fraud, see the respective call server documents on the [Avaya Support website](#). The phone cannot guarantee resistance to all Denial of Service (DoS) attacks. However, checks and protections are in-built to resist such attacks while maintaining appropriate service to legitimate users.

All IP phones that have WML Web applications support Transport Layer Security (TLS). The deskphone uses TLS to establish a secure connection to a HTTPS server, in which the upgrade and settings file can reside. The phone support TLS 1.2 cipher suites. You can configure the TLS_VERSION parameter to use either TLS 1.2 only, or use older TLS versions as well.

The following list of applications and processes use TLS 1.2:

- H.323 signaling over TLS
- SLA mon agent
- IPSec VPN with certificate based authentication
- 802.1x EAP-TLS
- Single Sign On (SSON)

- Configuration files download using HTTPS
- Backup/restore using HTTPS
- Debug report generation using HTTPS
- OCSP over HTTPS

*** Note:**

Because of POODLE vulnerability as defined in CVE-2014-3566, the IP phone do not support SSLv3.

If H.323 over TLS is enabled on the Communication Manager, the deskphone registers and opens a H.323 signaling over TLS connection by using TCP port 1300. Mutual authentication is supported and all registration and signaling packets are sent over TLS. The discovery messages are sent over UDP. You can disable H.323 signaling over TLS from the CRAFT menu.

All phones support HTTP authentication for backup and restore operations. The non-volatile memory stores the authentication credentials and the realm. The non-volatile memory is not overwritten if new phone software is downloaded. The default value of the credentials and the realm are null, set at manufacture and at any other time that user-specific data is removed from the phone or by the local administrative (Craft) CLEAR procedure.

A realm is the location of the user accounts. If you have set up a realm while installing the HTTPS server, the deskphone will prompt you to enter the realm address. For information about configuring realm, see the instructions provided by your HTTPS server vendor.

*** Note:**

If you have not configured realm, you can enter * in the **realm** field, and proceed.

If an HTTP backup or restore operation requires authentication and the realm in the challenge matches the stored realm, the stored credentials are used to respond to the challenge without prompting the user. However, if the realms do not match, or if an authentication attempt using the stored credentials fails, the user is then prompted to input new values for backup/restore credentials.

If an HTTP authentication for a backup or restore operation is successful and if the user ID, password, or realm used is different than the values currently stored in the phone, the new values will replace the currently stored values.

You also have the following options to restrict or remove how the deskphone displays crucial network information or uses the information.

- Support signaling channel encryption.

*** Note:**

Signaling and audio are not encrypted when unnamed registration is effective.

- Restrict the response of the phone to SNMP queries to only IP addresses on a list you specify.
- Specify an SNMP community string for all SNMP messages the phone sends.

- Apply the security-related parameters, SNMP community string (SNMPSTRING), SNMP Source IP addresses (SNMPADD), and Craft Access Code (PROCPSWD) that is administered on the call server. Download the file with encrypted signaling in addition to unencrypted HTTP or encrypted HTTPS.

 **Note:**

The phone supports the SNMPv2c protocol, which is not secure.

- Restrict dial pad access to Local Administration Procedures, such as specifying IP addresses, with a password.
- Restrict dial pad access to Craft Local Procedures to experienced installers and technicians.
- Restrict the ability of the user to use a phone Options application to view network data.
- Download and use third-party trusted certificates.

Registration and Authentication

Avaya call servers support using the extension and password to register and authenticate IP deskphones. For more information, see the current version of your call server administration manual.

Secure Shell Support

The phone supports the Secure Shell (SSH) v2 protocol. The SSH protocol is a tool that the Avaya services organization can use to remotely connect to IP deskphones to monitor, diagnose, or debug deskphone performance. Because of the sensitive nature of remote access, you can disable permission with the SSH_ALLOWED parameter.

The deskphone displays a security warning message at start of the session. You can specify your own file using SSH_BANNER_FILE, or the deskphone will use the following default file:

```
This system is restricted solely to authorized users for legitimate
business purposes only. The actual or attempted unauthorized access,
use, or modification of this system is strictly prohibited.
Unauthorized users are subject to company disciplinary procedures and
or criminal and civil penalties under state, federal, or other
applicable domestic and foreign laws. The use of this system may be
monitored and recorded for administrative and security reasons. Anyone
accessing this system expressly consents to such monitoring and
recording, and is advised that if it reveals possible evidence of
criminal activity, the evidence of such activity may be provided to
law enforcement officials. All users must comply with all corporate
instructions regarding the protection of information assets.
```

The Avaya technician can match the SSH fingerprint displayed under debug with the fingerprint present in the SSH client. This information is used to verify whether the administrator is logged on to the correct SSH server. The SSH fingerprint is not displayed when the FIPS mode is enabled. The deskphones support 2048-bit asymmetric key length for SSH server.

You can also administer the SSH_IDLE_TIMEOUT parameter to configure the duration of inactivity that will disable SSH.

Enhanced Authentication Security Gateway

Enhanced Authentication Security Gateway (EASG) is a challenge-response authentication and authorization solution used by Avaya service engineers. EASG is used to control the access and permissions of service engineers to the customer products.

The table below lists the EASG parameters and supported values:

Parameter name	Value	Description
EASG_SITE_AUTH_FACTOR	Null	Specifies Site Authentication Factor code associated with the EASG site certificate being installed. Valid values are 10 to 20 character alphanumeric string.
EASG_SITE_CERTS	Null	Specifies list of EASG site certificates which are used by technicians when they don't have access to the Avaya network to generate EASG responses for SSH login. The URLs must be separated by commas without any intervening spaces. Valid values are 0 to 255 ASCII characters.
CERT_WARNING_DAYS_EASG	365	Specifies how many days before the expiration of EASG product certificate that a warning should first appear on the phone screen. Syslog message will be also generated. Valid values are from 90 to 730.

Time-to-Service

The Time-to-Service (TTS) feature changes the way IP phones register with their gatekeeper, reducing the time to come into service.

In the absence of TTS, the system uses a coupled two-step procedure to bring the IP phones into service:

1. H.323 registration
2. TCP socket establishment for call signaling

The TTS feature separates these steps. You can enable IP phones for service with just the registration step. TCP sockets are established later, as needed.

The TTS feature also changes the direction of socket establishment. With TTS, Communication Manager, rather than the phone, initiates socket establishment, which further improves performance. You can enable TTS by default and can also disable TTS for all IP phones in a given IP network region by changing the IP Network form. TTS does not apply to the following phones: third party H.323, DCP, BRI, and analog.

The phone can accept an incoming connection request from a server on the gatekeeper list, use this new connection to replace an existing connection, and continue operation without the need to reregister. With this mechanism, Communication Manager starts a new connection to each deskphone during a server interchange. These phones then move quickly to the server and transition from the standby to active state.

TTS is supported with the following profiles:

- Challenge
- Annex-H
- H.323 signaling over TLS

TTS-TLS is not supported with the following features:

- IPsec VPN – only challenge and Annex-H are supported. H.323 over TLS is not supported over VPN.
- Unnamed registration

Communication Manager Administration

Related links

[Call server requirements](#) on page 98

[Call server administration](#) on page 99

[Call transfer administration](#) on page 102

[Call conferencing](#) on page 102

[Administering deskphones on Avaya Aura Communication Manager](#) on page 104

[Station administration](#) on page 106

[Aliasing phones for switch compatibility](#) on page 107

[Administering feature and call appearance labels](#) on page 107

Call server requirements

Before you perform administrative tasks, ensure that you have installed the proper hardware and your call server software is compatible with your phone. Use the latest PBX software and IP phone firmware.

Related links

[Communication Manager Administration](#) on page 98

Call server administration

For call server administration information not covered in this chapter, see the following documents on the [Avaya Support website](#) :

- *Administering Avaya Aura Communication Manager*, for more instructions for administering an IP phone system on Communication Manager.

For information on the process of adding new phones, see chapter 6, *Managing Telephones*. For related screen illustrations and field descriptions, see chapter on *Screen References*.

- *Administration for Network Connectivity for Avaya Communication Manager*, for more information about switch administration for your network.

Related links

[Communication Manager Administration](#) on page 98
[Administering the IP interface and addresses](#) on page 99
[Administering UDP port selection](#) on page 99
[Administering RSVP](#) on page 100
[Administering QoS](#) on page 100
[Administering IEEE 802.1Q](#) on page 100
[Administering DIFFSERV](#) on page 100
[Administering NAT](#) on page 100

Administering the IP interface and addresses

Follow these general guidelines:

- Define the IP interfaces for each CLAN and Media processor circuit pack on the call server that uses the IP Interfaces screen. For more information, see *Administration for Network Connectivity for Avaya Communication Manager*.
- On the Customer Options form, verify that the IP Stations field is set to **Y** (Yes). If it is not set to (Y), contact your Avaya sales representative. This guideline does not apply to the IP Softphone.

Related links

[Call server administration](#) on page 99

Administering UDP port selection

You can administer the phone from the Avaya Communication Manager Network Region which is form to support UDP port selection.

For information about Avaya Communication Manager implementation, see *Administration for Network Connectivity for Avaya Communication Manager*, on the [Avaya Support website](#).

Administer the switch to use a port within the proper range for the specific LAN, and the IP deskphone(s) copy that port. If no UDP port range is administered on the switch, the IP deskphone uses an even-numbered port, randomly selected from the interval 4000 to 10000.

Related links

[Call server administration](#) on page 99

Administering RSVP

The phone support the Resource Reservation Protocol (RSVP) for IPv4 audio connections only.

You can fully enable RSVP by provisioning CM ip-network-region.

Related links

[Call server administration](#) on page 99

Administering QoS

The IP deskphones support both IEEE 802.1D/Q and DiffServ.

Related links

[Call server administration](#) on page 99

Administering IEEE 802.1Q

The phone can simultaneously support receipt of packets that are tagged, or not tagged according to the IEEE 802.1Q standard. To support IEEE 802.1Q, you can administer phone from the network through LLDP, or by appropriate administration of the DHCP or HTTP/HTTPS servers.

You can administer the IEEE 802.1Q QoS parameters L2QAUD, and L2QSIG through the IP Network Region form. To set these parameters at the switch, see sections on *Quality of Service (QoS)* and *Voice quality administration* in *Administration for Network Connectivity for Avaya Communication Manager*.

Related links

[Call server administration](#) on page 99

Administering DIFFSERV

The DiffServ values change to the values administered on the call server as soon as the phone registers. Administer the DSCPAUD and DSCPSIG parameters to configure Diffserv for the deskphone. Unless there is a specific need in your enterprise LAN, do not change the default values.

Related links

[Call server administration](#) on page 99

Administering NAT

Network Address Translation (NAT) usage can lead to problems that affect the consistency of addressing throughout your network. All H.323 IP deskphones support NAT interworking. Support for NAT does not imply support for Network Address Port Translation (NAPT). The phones do not support communication to the PBX through any NAPT device.

NAT requires specific administration on the call server. A direct Avaya IP phone-to-Avaya IP phone call with NAT requires Avaya Communication Manager Release 3.0 or later software. For

more information, see *Administration for Network Connectivity for Avaya Communication Manager*, on the [Avaya Support website](#).

Related links

[Call server administration](#) on page 99

Administering Voice mail

Voice mail for deskphones with Communication Manager

When you press the **Messages** button, the deskphone first determines if the call server has a dedicated number for retrieving voice mail. If a dedicated number exists, the deskphone proceeds with voice mail retrieval.

Related links

[Communication Manager Administration](#) on page 98

Voice mail for deskphones aliased as 4600 Series IP Telephones

When native support does not apply, IP deskphones are aliased as 4600 Series IP telephones and run under CM Release 3.1 or later. In this case, use the `46xxsettings.txt` file to configure the **Messages** button by setting the system parameter MSGNUM to any dialable string.

Some MSGNUM examples:

- A standard telephone number the telephone should dial to access your voice mail system, such as AUDIX or Octel.
- A Feature Access Code (FAC) that allows users to transfer an active call directly to voice mail. FACs are supported only for QSIG-integrated voice mail systems like AUDIX or Octel. QSIG is an enhanced signaling system with which the voice mail system and Avaya Communication Manager Automated Call Processing (ACP) exchange information.

When the user presses the **Messages** button, the deskphone automatically dials the number or FAC, giving the user one-touch access to voice mail.

In the `46xxsettings.txt` file, specify the number to be dialed automatically when the user presses this button. The command is:

```
SET MSGNUM 1234
```

where `1234` is the Voice Mail extension for the CM hunt group or VDN.

Note:

You can use MSGNUM only when you alias the deskphone using non-native support. You must configure messaging for native support. A separate Voice Mail extension can be administered for each station.

Related links

[Communication Manager Administration](#) on page 98

Call transfer administration

This section provides information about call transfer behaviors to consider when you administer the call server. The phone application presents a user interface, based in part on the deduction of the call state. The following server-based features can interact with the user interface resulting in a call state that might need explanation:

- The system parameter **Abort Transfer?** is set to **Yes**. After you start a transfer, you cannot press a non-idle call appearance until the transfer is complete or the transfer is aborted.
- The system parameter **Abort Transfer?** is set to **No**: The transfer proceeds normally even if the user presses a non-idle call appearance before the transfer is complete.
- The system parameter **Transfer Upon Hang-up** is set to **No**: The user must press the **Complete** softkey after dialing the intended destination for the transfer to be completed.
- The system parameter **Transfer Upon Hang-up** is set to **Yes**: The user can hang up immediately after dialing and the transfer proceeds normally.

The features **Abort Transfer** and **Transfer Upon Hang-up** can interact. If a user initiates a transfer, dials the destination, and hangs up without pressing the **Complete** softkey, the three possible outcomes are:

- The transfer is completed. **Transfer Upon Hang-up** is set to **Yes**, regardless of the **Abort Transfer?** setting.
- The transfer is aborted. **Transfer Upon Hang-up** is set to **No** and **Abort Transfer?** is set to **Yes**.
- The transfer is denied. **Transfer Upon Hang-up** is set to **No** and **Abort Transfer?** is set to **No** and the call appearance of the transferee remains on soft hold.

Attempts to transfer an outside call to an outside line are denied. However, the user can drop the denied destination and initiate a transfer to an internal destination.

You can use the *Toggle Swap* feature to swap the soft-held and setup call appearances. That is, the setup call appearance becomes soft-held, and the soft-held call appearance becomes active as the setup call appearance. This feature works only once the setup call appearance is connected on a call. If *Toggle Swap* is pressed while the setup call appearance has ringback, the call server sends a broken flutter to the setup call appearance. If you press *Toggle Swap* while the setup call appearance is still dialing, *Toggle Swap* is ignored without a broken flutter. Toggle swapping the hold status of call appearances can be confusing to the user.

Related links

[Communication Manager Administration](#) on page 98

Call conferencing

This section provides information about conference call behaviors to consider when administering the call server. The deskphone application presents a user interface, based in part on the

deduction of the call state. The following call states might result when the server-based features interact with the user interface:

- The system parameter Abort Conference Upon Hang-up is set to **Yes**:

The user must dial and press the **Join** softkey for the conference to be completed. If the user hangs up during conference setup before pressing **Join**, the conference is cancelled with the held party remaining on [hard] hold. When the system parameter Abort Conference Upon Hang-up is set to **No**, the user can hang up immediately after dialing, dial a third party, and then press the **Join** softkey to have the conference proceed normally.

- The system parameter No Dial Tone Conferencing is set to **No** and the **Conference** or **Add** softkey is pressed:

The call server automatically selects an idle call appearance for the user to dial on. This action allows the user to add the next conferee. When the system parameter No Dial Tone Conferencing is set to **Yes**, the user must manually select a call appearance after pressing the **Conference** or **Add** softkey.

Conferencing behavior changes significantly when you set the Select Line Conferencing to **Yes**. Then the No Dial Tone Conferencing is automatically set to **Yes**. Specifically the following scenarios can occur:

- If the user finishes dialing the intended conferee, pressing the initial call appearance completes the conference, as if the **Join** softkey was pressed.
- If the user has not finished dialing the intended conferee, pressing the initial call appearance cancels the conference set up. Note: The initial conference is placed on soft hold when **Conference** or **Add** button is pressed.
- If the user presses the **Conference** or **Add** softkey, then immediately presses a hard-held call appearance, the previously held call appearance is retrieved from hold and joins the existing conference.

When you set the system parameter Select Line Conferencing to **No**, the user can cancel the conference setup by pressing the call appearance on soft hold before pressing **Join**. Selecting a hard-held call appearance during conference setup establishes the held call as the intended conferee.

For either Select Line Conferencing setting, if the user is in conference setup and answers an incoming call, the incoming call is established as the intended conferee. Then the user must press **Join** to add the answered call to the conference. If the user does not want the incoming call to be part of the conference, the user must not answer the call, or the user must answer the call and then hang up before continuing the conference setup. Pressing an in-use call appearance during conference setup makes that call appearance the intended conferee. The Toggle Swap feature works for Conference setup similar to Transfer Setup.

Related links

[Communication Manager Administration](#) on page 98

Administering deskphones on Avaya Aura® Communication Manager

This section covers Avaya Aura® Communication Manager administration on the Switch Administration Terminal (SAT) or by Avaya Site Administration. You must administer Avaya Aura® Communication Manager on SAT or by Avaya Site Administration to optimize the phone user interface. The SAT provides the system-wide CM form and the particular page or screen that you need to administer for each feature.

Related links

[Communication Manager Administration](#) on page 98

[Feature-related system parameters](#) on page 104

Feature-related system parameters

In Avaya Communication Manager, you can administer three system-wide parameters. When you administer these parameters on CM, the parameters are automatically downloaded to the phone during registration. You do not need to add these parameters using the `46xxsettings.txt` file or set them locally for each phone. The three system parameters are: SNMP community string, SNMP Source IP addresses, and Craft Access Code (PROCPSWD).

Note:

Commenting out SNMPSTRING in the `46xxsettings.txt` file will not prevent a response to an SNMP query unless the CM administration is also changed accordingly. Also, setting the SNMP flag on the IP-Options form in CM to "n" does not disable SNMP. You must enable the download flag and leave the community string value blank so that when the telephone registers, the SNMPSTRING value will remain null.

To administer these three parameters use Page 3 of the *change system-parameters ip-options form*.

Name	Description
On-hook Dialing on Terminals	Set up CM so that the phone supports on-hook dialing. Use the System Parameters Features form page 10. Use the command Change system-parameters features to view the form and make the change.
Auto Hold	Set up CM to enable Auto Hold, so that the phone automatically places an active call on hold when the user answers or resumes a call on another call appearance. Use the System Parameters Features form, page 6.

Table continues...

Name	Description
Coverage Path	Administer a coverage path for both phone demonstration and normal operations. Use the Coverage Path form and give it a number, for example, Coverage path 1. If Voice Mail is available, administer the hunt group or VDN, depending on the type of VM system being used.
Enhanced Conference Features	Enable enhanced conference display to support the user experience for conferences. Set Block Enhanced Conference Display on the Class of Restriction (COR) form to No. Use the command Change COR , followed by a number, to view the form and make the change. This is a sample of the Class of Restriction form.
EC500	Enable EC500 on the Off-PBX Telephones Station Mapping form if you have acquired the EC500 licenses. This feature requires trunking to work properly. Use the following command to make the change: change off-pbx-telephone station-mapping <station>
Wideband Audio	<p>Enable Wideband Audio, by using the change ip-codec-set <number> command on CM. Ensure that G.722–64K is first on the list of codecs. Note that wide band audio works only for direct-IP calls between two 96xx endpoints, either with both registered to the same server, or registered to different servers when connected by IP trunks. Calls between two 96xx phones connected by an IP trunk do not currently support wide band audio when the call is shuffled so that the media travels directly between the two phones. Calls that involve three or more parties, even if all parties use IP phones, do not use wide band. Calls between two phones where audio is terminated at a port network/gateway (PN/GW) media resource will not use wideband.</p> <p>Ensure that G.722 is added to all codec-sets that can possibly be used between all regions on the IP-Network Regions form . Technically, G722 does not need to be first. What is needed, however, is that all the non media processor-supported codecs (G722, SIREN, etc.) be placed before the media processor-supported codecs (G711, G729, G726, G723).</p> <p>For information on using the wideband codecs with the Communication Manager, see <i>Administering Avaya Aura® Communication Manager</i>, 03-300509.</p>

Related links

[Administering deskphones on Avaya Aura Communication Manager](#) on page 104

Station administration

Administer the following station features on the Station form in Avaya Aura® Communication Manager. The Station form comprises of several pages. You must set the features covered in this section to optimize the user interface.

The station form includes the field **Require Mutual Authentication if TLS**. This information implies whether the Communication Manager perform mutual authentication of the certificates in the case of the H.323 over TLS profile. If the field is set to *n*, the deskphone does not need the identity certificate. If the phone has an identity certificate, Communication Manager will request and verify the phone certificate signature using the trusted certificate repository. If the flag is set to *y*, the deskphone needs the identity certificate. The trusted certificate repository shall include the root CA certificate on the top of the trusted certificate chain of the identity certificate of the deskphone.

You can perform central call server administration of the GROUP parameter on a station-by-station basis. This parameter is then downloaded to each applicable deskphone starting with the next deskphone boot-up. You can use the GROUP Identifier with the `46xxsettings.txt` file for administration of specific groups of deskphones. You can administer the GROUP ID parameter on page 3 of the Change Station Form.

If applicable, before administering stations ensure that the phones are aliased according to the chart for Aliasing IP Deskphones for switch compatibility.

Related links

[Communication Manager Administration](#) on page 98

[Administering features](#) on page 106

Administering features

Administer the following Station Features for maximum user experience:

Name	Description
Enhanced Conference Features	Administer Conf-dsp (conference display) on the station form as a feature button. Users gain the benefits of enhanced conference features.
Auto select any idle appearance	Set Auto select any idle appearance to N (no) to optimize answering calls.

Related links

[Station administration](#) on page 106

Aliasing phones for switch compatibility

Avaya J100 Series IP Phones are not supported natively by Avaya Aura® Communication Manager and Avaya IP Office. You need to alias Avaya J100 Series IP Phones as 9611 phone on Avaya Aura® Communication Manager and Avaya IP Office.

Communication Manager supports J159/J169/J179/J189 H.323 IP phones. Avaya IP Office supports only Avaya J169/J179 IP Phone.

Related links

[Communication Manager Administration](#) on page 98

Administering feature and call appearance labels

You can administer feature / call appearance labels on the phone and button module using the Communication Manager Station form. The features administered on the Station form appear in the same sequence on the Feature screen of the phone and the button module.

Related links

[Communication Manager Administration](#) on page 98

Server Administration

Related links

[Software prerequisites](#) on page 107
[Administering the DHCP and file servers](#) on page 108
[DHCP generic setup](#) on page 109
[Setting up the DHCP server](#) on page 109
[Setting up a DHCPv6 server](#) on page 116
[HTTP generic setup](#) on page 116
[Backup and restore processing](#) on page 118
[About IPv4 and IPv6 operation](#) on page 120
[Features not supporting IPv6](#) on page 121

Software prerequisites

Ensure that you own licenses to use the DHCP, HTTP, and HTTPS server software.

Note:

You can install the DHCP and the HTTP server software on the same computer.



Caution:

The firmware in the IP Deskphones reserves the IP addresses of the form 192.168.2.x for internal communications. The phone might not function properly if you configure addresses in that range.

Related links

[Server Administration](#) on page 107

Administering the DHCP and file servers

Dynamic Host Configuration Protocol (DHCP) minimizes maintenance for the IP Telephone network. With DHCP, you need not individually assign and maintain IP addresses and the other parameters on each IP phone on the network.

Depending on administration, the DHCP server provides the following information to the IP Telephones:

- An IP address of the IP Telephone
- An IP address of the Avaya call server
- An IP address of the HTTP or HTTPS file server
- The subnet mask
- An IP address of the router
- A DNS Server IP address

Administer the LAN so each IP deskphone can reach a DHCP server that contains the IP addresses and subnet mask.

The phone cannot function without an IP address. Using the IP address reuse capability, the phone can reuse the previous IP address and parameter settings even if the DHCP server is temporarily unavailable. A user can manually assign a different IP address to an IP deskphone. When the DHCP server finally returns, the phone does not search for a DHCP server unless the static IP data is unassigned manually. In addition, manual entry of IP data is an error-prone process.

Ensure that:

- A minimum of two DHCP servers are available for reliability.
- A DHCP server is available when the IP deskphone restarts.
- A DHCP server is available at remote sites if WAN failures isolate IP deskphones from the central site DHCP servers.

The file server provides the phone with a script file and, if appropriate, new or updated application software.

In addition, you can edit the settings file to customize phone parameters for your specific environment.

Related links

[Server Administration](#) on page 107

DHCP generic setup

This document describes the generic DHCPv4 and DHCPv6 administration that works with the IP Deskphones.

Windows operating systems include several DHCP software alternatives such as:

- Windows 2008® DHCP Server
- Windows 2012® DHCP Server

Any DHCP application might work if the DHCP server is correctly configured.

 **Note:**

Avaya does not assume responsibility for configuring your DHCP server. Contact your vendor or supplier for configuring the DHCP server correctly.

Related links

[Server Administration](#) on page 107

Setting up the DHCP server

About this task

DHCP server setup involves:

Procedure

1. Follow vendor instructions to install the DHCP server software.
2. Configure the DHCP server with:
 - IP addresses available for the phone.
 - The following DHCP options for using IPv4:
 - **Option 1: Subnet mask.**
 - **Option 3: Gateway (router) IP addresses.** If using more than one address, the total list can contain up to 255 total ASCII characters. You must separate IP addresses with commas with no intervening spaces.
 - **Option 6: DNS servers address list.** If using more than one address, the total list can contain up to 127 total ASCII characters. You must separate IP addresses with commas with no intervening spaces. At least one address in Option 6 must be a valid, dotted decimal address without a zero.
 - **Option 15: DNS Domain Name.** This string contains the domain name that the system uses to resolve DNS names in system parameters into IP addresses. The

system appends this domain name to the DNS name before the IP Deskphone resolves the DNS address. If you want to use a DNS name for the HTTP server, Option 15 is required. Otherwise, you can specify a DOMAIN as part of customizing HTTP. For more information, see [DNS addressing](#) on page 168.

- **Option 43: Encapsulated vendor-specific options.** This option is used by the deskphones and the DHCP servers to exchange vendor-specific information. The following table lists the codes supported by the deskphones and the corresponding `46xxsettings.txt` parameters:

Code	Parameter
1	Must be the first encapsulated parameter in Option 43 with a value of 6889. * Note: Option 43 is processed only if the first code is 1 with a value of 6889, where 6889 is the enterprise identifier.
2	HTTPSRVR
3	HTTPDIR
4	HTTPPORT
5	TLSSSRVR
6	TLSDIR
7	TLSPORT
9	L2Q
10	L2QVLAN
11	PHY1STAT
12	PHY2STAT
13	PROCSTAT
14	SIG
16	MCIPADD
17	TLSSSRVRVERIFYID

* **Note:**

The deskphone sends DHCP option 60 with the value `ccp.avaya.com`.

- **Option 51: DHCP lease time.** If the deskphone does not receive this option, the deskphone does not accept the DHCPOFFER. Avaya recommends a lease time of six weeks or greater. If this option has a value of FFFFFFFF hex, the system treats the IP address lease as infinite as required by RFC 2131, Section 3.3. In this case, the deskphone does not require renewal and rebinding procedures even if you receive Options 58 and 59.

Expired leases cause IP Deskphones to restart. Avaya recommends providing enough leases so the IP address of a IP deskphones does not change if you briefly take the phone offline.

 **Note:**

The DHCP standard states that when a DHCP lease expires, the device must immediately cease using the assigned IP address. However, if the network has problems and the you centralize the DHCP server, or if the DHCP server has problems, the deskphone does not receive responses to its request for a renewal of the lease. In this case the deskphone is unusable until the server can respond. Expired leases do not cause the phone to restart because you can renew expired leases. However, if the new IP address is different than the previous, the phone restarts. Ensure that after an IP address is assigned, the deskphone continues using that address after the DHCP lease expires, until the system detects a conflict with another device. With the system parameter DHCPSTD, an administrator can specify that the telephone will do one of the following: a). Comply with the DHCP standard by setting DHCPSTD to 1. b). Continue to use the IP Address after the DHCP lease expires by setting DHCPSTD to 0. This setting is the default. If you invoke the default after the DHCP lease expires, the phone continues to broadcast DHCPREQUEST messages for the current IP address. The deskphone sends an ARP Request for its own IP Address every 5 seconds until the phone receives a DHCPACK, a DHCPNAK, or an ARP Reply. After receiving a DHCPNAK, or ARP Reply, the phone displays an error message, sets the IP address to 0.0.0.0, and attempts to contact the DHCP server again. Depending on the DHCP application you choose, be aware that the application does not immediately recycle expired DHCP leases. An expired lease might remain reserved for the original client for one day or more.

The following example shows the implication of having a reservation period: Take two IP addresses, therefore two possible DHCP leases. Take three IP deskphones, two of which are using the two available IP addresses. When the lease for the first two deskphones expires, the third deskphone cannot get a lease until the reservation period expires. Even if you remove the other two deskphones from the network, the third deskphone remains without a lease until the reservation period expires.

- **Option 52: Overload Option**, if required. If the IP deskphones receives this option in a message and interprets the *sname* and *file* fields in accordance with IETF RFC 2132, Section 9.3.
- **Option 58: DHCP lease renew time**. If the IP deskphones does not receive this parameter, or if this value is greater than that for Option 51, the phone uses the default value of T1 (renewal timer) according to IETF RFC 2131, Section 4.5.
- **Option 59: DHCP lease rebind time**. If the IP deskphones does not receive this parameter, or if this value is greater than that for Option 51, the phone uses the default value of T2 (rebinding timer) according to RFC 2131, Section 4.5
- **Option 242: Site-Specific Option Number (SSON)**. You do not have to use Option 242. If you do not use this option, you must ensure that you administer the key information, especially HTTPSRVR and MCIPADD appropriately elsewhere.

An example of proper DHCP administration is:

Option 242 for DHCP: **MCIPADD** =xxx.xxx.xxx.xxx

Result

In the following table, the IP deskphones sets the following parameter values to the DHCPACK message field and option.

Table 8: DHCPACK Setting of Parameter Values

Parameter	Set to
DOMAIN	If received, Option #15.
DHCP lease renew time	Option #58 (if received).
DHCP lease rebind time	Option #59 (if received).
DHCP lease time	Option #51 (if received).
DNSSVR	Option #6.
HTTPSRVR	The siaddr field, if that field is not a zero.
TLSSVR	The siaddr field, if that field is non zero.

Because the DHCP site-specific option is processed after the DHCP fields and standard options, the values set in the site-specific option supersede any values set by DHCP fields or standard options, as well as any other previously set values.

You cannot set parameters L2Q, L2QVLAN, and PHY2VLAN from a *site-specific option* if the parameter values were previously set by LLDP.

* Note:

The phone do not support Regular Expression Matching, and therefore, do not use wildcards.

In configurations where the upgrade script and the application files are in the default directory on the HTTP server, do not use the command HTTPDIR=<path>.

Related links

[Server Administration](#) on page 107

[Configuring a DHCP server in the dual and IPv6-only environments](#) on page 112

[Configuring DHCP Option 242](#) on page 113

Configuring a DHCP server in the dual and IPv6-only environments

About this task

In the dual (IPv4 and IPv6) and IPv6-only environments, the phone acquires vendor-specific parameters, including the IP address of the file server, through DHCPv6 vendor-specific option 17. Use this procedure to set this option with an opt-code 242 to obtain an IPv6 address for the file server.

Before you begin

In the dual environment, install the DHCPv4 and DHCPv6 server software according to instructions provided by your vendor.

In the IPv6-only environment, install the DHCPv6 server.

Procedure

1. Depending on the environment, do one of the following:
 - In the dual environment, specify the IP address of the file server using DHCPv4.
 - In the IPv6-only environment, specify the IP address of the file server using DHCPv6.
2. Configure the DHCPv6 server to send a Vendor-Specific Information (VSI) option with an enterprise number of 6889 which is the Avaya Enterprise Number.
3. Include the vendor-specific option 17 with an opt-code of 242 within that option.
4. Set the option-data portion of the vendor-specific option with the HTTPSRVR parameter.

Example

The following shows an example of setting the vendor-specific option 17 in the `dhcp6.conf` file:

```
## SSON on Avaya phone default is 242
## Specific the HTTP server used by the Avaya phones

## Allocate 2 bytes for option code, 2 bytes for option data length, 3 hash buckets
option space Avaya code width 2 length width 2 hash size 3;
option Avaya.avaya-option-242 code 242 = text;

## 6889 is enterprise number for Avaya
option vsio.Avaya code 6889 = encapsulate Avaya;

## option data (sample):
option Avaya.avaya-option-242
"HTTPSRVR=2000::114f:85f7:f238:9eb5,MCIPADD=2000::54,SIG=SIP";
```

Next steps

In the dual environment, it is recommended to set DUAL_IPPREF to 6 to override the default value of 4 in the `46xxsettings.txt` file.

This parameter is used only in dual mode to apply Site Specific Option Number (SSON) parameters either from a DHCPv4 or a DHCPv6 server.

Related links

[Setting up the DHCP server](#) on page 109

Configuring DHCP Option 242

About this task

To administer DHCP option 242 for SSON, make a copy of the existing option 176 for your IP deskphones. Option 242 is specific to the default site and applies to DHCPv4 only. You can then perform one of the following actions:

Procedure

1. Ignore any parameters which the IP Deskphones do not support for setting through DHCP in option 242, or
2. Delete unused or unsupported IP Deskphone parameters to shorten the length of the DHCP message.

Result

You can set only the following parameters in the DHCP site-specific option for IP Deskphones, although most of them can be set in a `46xxsettings.txt` file as well.

Table 9: Parameters Set by DHCP in a Site-Specific Option

Parameter	Description
DNSSRV	Specifies the DNS server IP address or addresses.
DOMAIN	Specifies the string that is appended to DNS names in parameter values when they are resolved into IP addresses.
DOT1X	Controls the operational mode for 802.1X. The default is 0, for pass-through of multicast EAPOL messages to an attached PC, and enables Supplicant operation for unicast EAPOL messages.
DOT1XSTAT	Controls 802.1X Supplicant operation.
HTTPDIR	Specifies the path name to prepend to all file names used in HTTP and HTTPS GET operations during startup. (0 to 127 ASCII characters, no spaces.) The command is <i>SET HTTPDIR myhttpdir</i> . The path relative to the root of the TLS or HTTP file server where IP Deskphones files are stored. If an Avaya file server is used to download configuration files over TLS, but a different server is used to download software files through HTTP, set the path of the Avaya server in the DHCP site-specific option, and set HTTPDIR again in the <code>46xxsettings.txt</code> file with the appropriate path for the second server. HTTPDIR is the path for all HTTP operations except for BRURI.
HTTPPORT	Specifies the TCP port number for downloading files from HTTP file server.
HTTPSRV	Specifies the IP addresses or DNS names of HTTP file servers used to download IP Deskphones software files. The files are digitally signed, so TLS is not required for security.
ICMPDU	Controls the extent to which ICMP Destination Unreachable messages are sent in response to messages sent to closed ports so as not to reveal information to potential hackers. The default is 1 which sends Destination Unreachable messages for closed ports used by traceroute.
ICMPRED	Controls whether ICMP Redirect messages are processed. The default is 0 which redirects messages that are not processed.
L2Q	specifies the 802.1Q tagging mode. The default is 0 which signifies automatic.
L2QVLAN	VLAN ID of the voice VLAN. The default is 0.
LOGLOCAL	Controls the severity level of events logged in the SNMP MIB. The default is 7.
MCIPADD	CM servers IP addresses or DNS names. If there are too many addresses or names to include all of them in the DHCP site-specific option, include at least one from each major system. Then set MCIPADD again in the <code>46xxsettings.txt</code> file with the complete list of addresses. Providing a subset of the addresses through DHCP improves reliability if the file server is not available due to server or network problems.
NDREDV6	NDREDV6 IPv6 only. Controls whether IPv6 Neighbor Discovery Redirect messages will be processed.

Table continues...

Parameter	Description
PHY1STAT	Controls the Ethernet line interface speed. The default is 1 which indicates that it is auto-negotiate.
PHY2STAT	Controls the secondary Ethernet interface speed. The default is 1 which indicates that it is auto-negotiate.
PROCPSWD	Security string used to access local procedures. The default is 27238 (CRAFT).
PROCSTAT	Controls whether local Craft procedures are allowed. The default is 0 which indicates that access to all administrative options is allowed.
REREGISTER	The number of minutes the phone waits before and between re-registration attempts.
REUSETIME	The number of seconds to wait for successful completion of DHCP before reusing previous parameters on the default (port) VLAN. The default is 60.
SIG	The signaling protocol download flag that indicates which protocol applies (H.323 (1), SIP, (2) or Default (0). For software releases prior to 6.0, SIG can only be set manually on the deskphone and not through DHCP or in the <code>46xxsettings.txt</code> file. Default means the default protocol supported at that location. A custom upgrade file is required to support both protocols. For software releases 6.0 and later, separate upgrade files with different names are used for H.323 and SIP, and Default means to download the upgrade file for the same protocol that is supported by the software that the deskphone is currently using.
SNMPADD	Allowable source IP addresses for SNMP queries. The default is " " (Null).
SNMPSTRING	SNMP community name string. The default is " " (Null).
STATIC	Controls whether to use a manually-programmed file server or CM IP address instead of those received through DHCP or the <code>46xxsettings.txt</code> file. If a manually programmed file server IP address is to be used, STATIC must be set through DHCP.
TLSDIR	Specifies the path name prepended to all file names used in HTTPS GET operations during startup.
TLSPORT	Specifies the TCP port number for downloading files from HTTPS file server.
TLSSRV	Specifies the IP addresses or DNS names of Avaya file servers to download configuration files. Specifies that Transport Layer Security is used to authenticate the server.
UNNAMEDSTAT	Specifies whether the deskphone will attempt unnamed registration.
VLANTEST	Controls the length of time the deskphone tries DHCP with a non-zero VLAN ID. When the interval is exceeded, the deskphone records the VLAN ID so that the VLAN ID is not used again, and DHCP continues on the default VLAN. The default is 60 seconds.

These parameters are saved in the non-volatile memory of the IP Deskphones. If the DHCP server is not available for any reason during phone restart or reboot, the phone uses these saved parameters.

Related links

[Setting up the DHCP server](#) on page 109

Setting up a DHCPv6 server

About this task

Important:

Avaya does not support IPv6 for the general market, and makes the software available to a specific set of customers with known limitations. Any additional limitation or bugs discovered within this release will be considered for resolution in future major releases.

To set up the DHCPv6 server:

Procedure

1. Install the DHCP server software according to vendor instructions.
2. Configure the DHCP server to send a Vendor-Specific Information (VSI) option with an enterprise number of 6889 which is the Avaya Enterprise Number.
3. Include the vendor-specific option with an opt-code of 242 within that option.
4. Set the option-data portion of the vendor-specific option with the applicable parameters. For information about the parameters, see the site-specific DHCP options.

Additionally, the parameters DOMAIN and DNSSRV can be set in other numbered options by DHCP. These parameters can also be set in the Avaya DHCPv6 vendor-specific option.

Result

The vendor-specific option is processed after the DHCP fields and standard options. As such, any values set using the VSI will supersede any values that are set using DHCP fields or standard options, as well as any other previously set values.

Related links

[Server Administration](#) on page 107

HTTP generic setup

About this task

You can store the same application software, script file, and the `46xxsettings.txt` file on an HTTP server. The phone uses the application software, script file, and the `46xxsettings.txt` file. The phone might lose some functionality, if you reset the HTTP server or the HTTP server is unavailable. MVIPTL and IIS6 are not supported with HTTPS. When using HTTPS, before upgrading, you must replace the server.

Caution:

Ensure that the files defined by the HTTP server configuration are accessible from all IP Deskphones that need those files. Ensure that the file names match the names in the upgrade script, including case, as UNIX systems are case-sensitive.

*** Note:**

Use any suitable HTTP application. Commonly used HTTP applications include Apache® and Microsoft® IIS™.

To use HTTPS, you must download the trusted certificates to the phone, by using the TRUSTCERTS parameter. The deskphone authenticates the server certificate. If the HTTPS server is provided by Avaya and the HTTPS server certificate has Avaya Product root CA, the deskphone cannot download files and perform Backup/restore to this server, without downloading trusted certificates. Set AUTH to 1 to force downloading configuration files from the HTTPS server. After you set AUTH to 1, the deskphone downloads configuration files from servers which have server certificate with a corresponding root certificate in the phone trusted certificates repository.

To set up an HTTP server:

Procedure

1. Install the HTTP server application.
2. Administer the system parameter HTTPSRVR to the addresses of the HTTP server.
Include the parameter in DHCP Option 242, or the appropriate SSON Option.
3. Download the upgrade script file and application files from the [Avaya Support website](#) to the HTTP server.

For more information, see [Telephone Software and Application Files](#) on page 122.

*** Note:**

When you download the application file from the [Avaya Support website](#), ensure you are downloading the correct version. One version allows VPN and media encryption functionality, while the other disables those functions.

*** Note:**

IP phone H.323 v 6.6.2 and later do not support HTTPS with MV_IPTTEL or IIS 6. It is recommended to upgrade to the current version of an HTTPS server that supports TLS 1.2.

Result

If you choose to enhance the security of your HTTP environment by using Transport Layer Security (TLS), you must:

- Install the TLS server application. Use of TLS for HTTPS also means download and configuration of TRUSCERTS with the customer root CA used for signing the HTTPS server identity certificate.
- Administer the system parameter TLSSRV to the addresses of the Avaya HTTPS server.

Related links

[Server Administration](#) on page 107

[HTTP Redirect feature](#) on page 118

HTTP Redirect feature

HTTP redirection allows you to configure and use multiple servers to download files to IP phones without the need to configure different values of HTTPSRVR (or TLSSRV) for different groups of phones.

You do not need any special configuration on the phone. The phone responds automatically to HTTP redirection requests from the HTTP server.

Using this feature you can:

- Spread the load across multiple servers. This feature allows local file servers to be used to avoid bottlenecks caused by low bandwidth WAN links to remote locations.
- Use this capability for firmware upgrades, backup or restore and agent greeting download.

The feature supports the following HTTP Redirection response codes:

- 301 (Moved Permanently)
- 302 (Found)
- 303 (See Other)
- 307 (Moved Temporarily)

To be able to use this feature, you must configure the central file server to support HTTP Redirection to an appropriate alternate server. See the [Microsoft](#) website for more information and examples on configuring HTTP Redirection on IIS7 server.

Related links

[HTTP generic setup](#) on page 116

Backup and restore processing

IP deskphones support the HTTP client to back up and restore the user-specific data. The deskphones support HTTP over TLS (HTTPS) for backup or restore. For backup, the deskphone creates a file with all user-specific data if a backup file location is specified in system parameter BRURI. The file is sent to the server by an HTTP PUT message, with appropriate success or a failure confirmation.

Note:

IP phone H.323 v6.6.2 and later do not support HTTPS with MV_IPTTEL or IIS 6. It is recommended to upgrade to the current version of an HTTPS server that supports TLS 1.2.

The phone stores the authentication credentials and the realm in non-volatile memory that is not overwritten if new phone software is downloaded. The default value of the credentials and the realm is set to null at manufacture and at any other time that user-specific data is removed from the deskphone.

For restore, the initiating process must supply only the backup file name. The file is requested from the server by an HTTP GET message. If successful, the file is returned to the initiating process. Otherwise a failure message is returned.

Backup and restore operations construct the URI used in the HTTP message from the value of the BRURI parameter and from the file name as follows:

- If BRURI ends with a / (a forward slash), the file name is appended.
- Otherwise, a forward slash and the file name is appended to the BRURI value.

 **Note:**

BRURI can include a directory path and or a port number as specified in IETF RFCs 2396 and 3986.

For backup, the initiating process must supply the backup file and the file name, and the file is sent to the server through an HTTP PUT message. A success or failure indication is returned to the initiating process based on whether or not the file is successfully transferred to the server.

For restore, the initiating process must only supply the file name, and the file is requested from the server through an HTTP GET message. The file is returned to the initiating process if it is successfully obtained from the server, otherwise a failure indication is returned.

If you use TLS, the call server registration password for the phone must be included in an Authorization request-header in each transmitted GET and PUT method. This method is intended for use by the Avaya IP Telephone File Server Application so that the phone requesting the file transaction can be authenticated. You can download the Avaya IP Telephone File Server Application from the [Avaya Support website](#).

If no digital certificates are downloaded based on the system parameter TRUSTCERTS, the phone establishes a TLS connection only to a backup and restore file server that has a Avaya-signed certificate. The Avaya certificate is included by default with the Avaya IP Telephone File Server Application, and includes the credentials. However, if at least one digital certificate has been downloaded based on TRUSTCERTS, the credentials are included only if BRAUTH is set to 1. This method is a security feature to allow control over whether the credentials are sent to servers with third-party certificates. If the server on which the Avaya IP Telephone File Server Application is installed uses a non-Avaya certificate, set BRAUTH to 1 to enable authentication of the deskphones. The default value of BRAUTH is 0.

When the call server IP address and the registration password of the phone are included as the credentials in an Authorization request-header, the call server IP address is included first in dotted-decimal format, followed by a colon, hex 3A, followed by the registration password of the phone.

When the call server IP address and the registration password of the phone are included as the credentials in an Authorization request-header, the call server IP address is included first in dotted-decimal format, followed by a colon (hex 3A), followed by the registration password of the phone. The server gets the extension number of the phone from the backup or restore file name. The server must also protect the user's credentials once they are received through the secure TLS connection.

The phone sends the registration credentials without regard to the BRAUTH setting if no certificates are downloaded. Only server certificates signed by an Avaya Root CA certificate are authenticated if no certificates are downloaded.

If an HTTP backup or restore operation requires authentication and the realm in the challenge matches the stored realm, the phone uses the stored credentials to respond to the challenge without prompting the user. However, if the stored credentials are null, or if the realms do not match, or if an authentication attempt using the stored credentials fails, the Status Line of the IP Deskphones or the Prompt Line for all other IP Deskphones display an HTTP Authentication or an HTTP Authentication Failure interrupt screen: `Enter authentication credentials.`

New values replace the stored authentication and realm values:

- When HTTP authentication for backup or restore succeeds
- If the userid, password, or realm used differs from those values that are stored in the phone
- If HTTP authentication fails, the user is prompted to enter new credentials.

 **Note:**

The HTTP basic authentication method is not secure. Use this method only for compatibility with file servers that require authentication. For example, IIS 7.0 and later require authentication for PUT requests. Volume settings for the ringer and the speaker are persistent after reboot and backup/restore.

 **Note:**

Users can request a backup or restore using the **Advanced Options > Backup/Restore** screen, as described in the user guide for their specific deskphone model.

Related links

[Server Administration](#) on page 107

About IPv4 and IPv6 operation

 **Important:**

Avaya does not support IPv6 for the general market, and makes the software available to a specific set of customers. Any additional limitation or bugs discovered within this release will be considered for resolution in future major releases.

From Release 6.0 onwards, Internet Protocol (IP) operation determination follows this order:

- If NVVPNMODE parameter value is set to 1 (Yes) only IPv4 operation is enabled.
- If NVVPNMODE is set to 0 (No), the IPv6 status IPV6STAT parameter is checked to see if IPv6 is allowed; if set to 0 (No) then only IPv4 operation is enabled.
- If IPV6STAT is set to 1 (support IPv6), then the DHCPSTAT parameter is checked:
 - If DHCPSTAT is set to 1 (use DHCPv4 only) then IPv4 only is enabled. But if an IPv6 address was manually programmed, dual-stack operation is enabled.
 - If DHCPSTAT is set to 2 (use DHCPv6 only) then IPv6 only is enabled. But if an IPv4 address was manually programmed, dual-stack operation is enabled.
 - If DHCPSTAT is set to 3 (both IPv4 and IPv6 supported), then dual-stack operation is enabled.

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

If IPv6-only operation is enabled, any IPv4 addresses configured as parameter values are ignored, and the next IPv6 address (if any) in a list of addresses is used. If the parameter value does not contain any IPv6 addresses, the system treats the value as null.

The results of the determination are expressed in the following table.

Table 10: IP Enablement Results

Manually program- med IPv4 address?	IPV6STAT	Manually programmed IPv6 address	DHCPSTAT	Result	Addressing Mode(s)	
					IPv4	IPv6
No	0	N/A	n/a	IPv4 only	DHCP	n/a
	1	No	1	IPv4 only	DHCP	n/a
		Yes	2	IPv6 only	n/a	DHCPv6
			3	dual-stack	DHCP	DHCPv6
			1 or 3	dual-stack	DHCP	manual
			2	IPv6 only	n/a	manual
Yes	0	n/a	n/a	IPv4 only	manual	n/a
	1	No	1	IPv4 only	manual	n/a
		Yes	2 or 3	dual-stack	manual	DHCPv6
			n/a	dual-stack	manual	manual

In general, if dual-stack operation is enabled, whether IPv4 or IPv6 is to be used to contact a server is determined by the value of the parameter that contains the server address(es). However, if the value is a DNS name and if DNS returns both an IPv4 and an IPv6 address, the one that will be used is controlled by the parameter IPPREF.

Related links

[Server Administration](#) on page 107

Features not supporting IPv6

The features and capabilities detailed in the following table are not available with IPv6 in H.323 software Release 6.0 or later:

Table 11: Features not supporting IPv6

VPN [IPsec, IKEv1]	LLDP	RSVP [IPv4 audio connections only]	RTP
RTCP Monitoring	CNA	HTTP Server Push Request	Certificates
Syslog	DHCP	Remote Trace Route, Remote Ping	Audio Push
SSH	SNMP	Dynamic VLAN	PTI
Many debugging and reporting capabilities available for IPv4	DOS attack blocker	All secure protocols, including but not limited to https, secure BR, agent greetings	

 **Note:**

Avaya does not support IPv6 for the general market, and makes the software available to a specific set of customers with the understanding that IPv6 is undergoing further refinement. It is strongly recommended that customers planning to deploy IPv6 first thoroughly evaluate it in a test environment that mimics the target live environment. IPv6 environments requiring capabilities detailed in the table above are not supported with this release. Any additional limitation or bugs discovered within this release will be considered for resolution in future major releases.

Related links

[Server Administration](#) on page 107

Telephone Software and Application Files

Related links

[Understanding the general download process](#) on page 122

[Using the GROUP parameter to set up customized groups](#) on page 125

Understanding the general download process

IP Deskphones download upgrade files, settings files, language files, certificate files, and software files from a file server. IP deskphone downloads all the file types either through HTTP or HTTPS except the software files, which can only be downloaded through HTTP. Avaya recommends HTTPS for downloading the non software file types because it ensures the integrity of the downloaded file by preventing *man in the middle* attacks. Further, after the deskphone downloads the trusted certificates, HTTPS ensures that the file server is authenticated through a digital certificate. The deskphone does not use HTTPS for software file downloads because IP

deskphones software files are already digitally signed. You need not incur additional processing overhead while downloading these relatively large files.

*** Note:**

The files in the Software Distribution Packages discussed in this chapter are identical for file servers running HTTP and HTTPS. The generic term, file server, refers to a server running either HTTP or HTTPS.

IP phone H.323 v6.6.2 and later do not support HTTPS with MV_IPTTEL or IIS 6. It is recommended to upgrade to the current version of an HTTPS server that supports TLS 1.2.

When shipped from the factory, IP deskphones might not contain the latest software. When you first plug in the IP deskphone, the phone attempts to contact a file server, and downloads new software only if the software version available on the file server is different than the version on the phone. For subsequent software upgrades, the call server can remotely reset the phone, and the phone initiates the same process for contacting a file server.

The phone queries the file server, which, transmits a 96x1Supgrade.txt file (SIP protocol) or 96x1Hupgrade.txt file (H.323 protocol) to the deskphone based on the SIG parameter setting. The software files that the deskphone must use depend on the instructions in the upgrade file.

The following HTTP servers support upgrade and downgrade when FIPS is enabled on the phone.

- Apache
- IIS 6
- IIS 7.0 and later
- IIS 8
- IIS 10.0
- Utility Server

! Important:

The MV_IPTTEL server does not support upgrade or downgrade when FIPS is enabled on the phone.

The phone then downloads the 46xxsettings.txt file. The settings file contains options that you have administered for any or all the phones in your network. After downloading the 46xxsettings.txt file, the phone downloads the language or the certificate files and then any new software files that the settings require.

Related links

[Telephone Software and Application Files](#) on page 122

[Choosing the right application file and upgrade script file](#) on page 124

[Using the upgrade file](#) on page 124

[About the settings file](#) on page 124

Choosing the right application file and upgrade script file

Software files required to operate the phone are packaged together in either a Zip format or RPM/Tar format distribution package. Download the package appropriate to your operating environment to your file server from the [Avaya Support website](#).

The choice of the package depends on the protocol you are using, H.323 or SIP, for all or the majority of your phones.

H.323 software distribution packages contain:

- One upgrade file
- All of the display text language files
- A file named `av_prca_pem_2033.txt` that contains a copy of the Avaya Product Root Certificate Authority certificate in PEM format that may be downloaded to telephones based on the value of the TRUSTCERTS parameter
- A file named `release.xml` that is used by the Avaya Utility Server.

Release 6.0 and later software distribution packages in Zip format also contain a signatures directory containing signature files and a certificate file to be used by the Avaya file server application on the Utility server. Customers using a non-Avaya HTTP server can ignore or delete this directory.

Related links

[Understanding the general download process](#) on page 122

Using the upgrade file

The upgrade file indicates to the phone whether it needs to upgrade software. From Release 6.0 onwards, the upgrade file is either H.323-specific or SIP-specific. The deskphones read this file whenever the deskphone is reset. The upgrade script file also directs the phone to the settings file.

Avaya recommends that you do not alter the upgrade script file because if Avaya changes the upgrade script file in the future, any changes you have made will be lost. Avaya recommends that you use the `46xxsettings.txt` file to customize your settings instead. However, you can change the `46xxsettings.txt` file name, if desired, as long as you also edit the corresponding `GET` command in the upgrade file script.

Related links

[Understanding the general download process](#) on page 122

About the settings file

The settings file contains the option settings you need to customize the IP deskphones for your enterprise.

Note:

You can use one settings file for all your Avaya IP deskphones.

The settings file can include any of six types of statements, one on each line:

- Tag lines that begin with a single **#** (pound) character, followed by a single space character, followed by a text string with no spaces.
- **Goto** commands, of the form `GOTO tag`. **Goto** commands cause the phone to continue interpreting the settings file at the next line after a `#tag` statement. If no such statement exists, the rest of the settings file is ignored.
- Conditionals, of the form `IF $parameter_name SEQ string GOTO tag`. Conditionals cause the **Goto** command to be processed if the value of the parameter named *parameter_name* exactly matches *string*. If no such parameter named *parameter_name* exists, the entire conditional is ignored. You can use only the following parameters in a conditional statement are: GROUP, MACADDR, MODEL, MODEL4, VPNACTIVE and SIG_IN_USE.
- **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, even if the value itself is numeric, a dotted decimal IP Address, etc.
- Comments, which are statements that start with either two pound characters (**##**) or one pound (**#**) character followed by any character except space, in the first column.

 **Note:**

The pound (**#**) character followed by a space represents a tag, and not a comment.

Download the `46xxsettings.txt` template file from the [Avaya Support website](#) and edit it to add your own custom settings.

Related links

[Understanding the general download process](#) on page 122

Using the GROUP parameter to set up customized groups

About this task

Different users might have the same phone model, but require different administered settings. For example, you might want to restrict call center agents from logging off, which might be an essential capability for *hot-desking* associates.

Use the GROUP parameter to set up customized groups:

Procedure

1. Identify the phones and the groups the phones belong to, 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 is assigned as Group 0.

2. You can only set the GROUP parameter either at each individual deskphone or when you register a phone with Avaya Aura[®] Communication Manager.

To set the GROUP parameter on each deskphone, use the GROUP procedure from the local administrative options. To set the GROUP parameter on a phone registered with Communication Manager, administer the GROUP parameter on a phone-by-phone basis on the Communication Manager Station Form.

3. After you assign the GROUP assignments, edit the configuration file to enable each phone of the appropriate group to download the proper settings.

Result

The following is an example of the configuration file for the call center agent:

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

Related links

[Telephone Software and Application Files](#) on page 122

Administering Deskphone Options

Administering options

This chapter explains how to change parameter values by using the DHCP or HTTP servers and provides additional information about some related features.

You can set the parameters for DHCP, DHCP fields, and options to the required values. For HTTP, set the parameters to required values in the settings file.

Use the settings file to administer most parameters on the H.323 Deskphones. Some DHCP applications are complicated and require extensive expertise for administration.

You might choose to completely disable the capability to enter or change option settings from the dial pad. You can set the parameter PROCPSWD as part of standard DHCP/HTTP administration. Alternately, you can set PROCPSWD on the system-parameters ip-options form, in Communication Manager Release 4.0. If PROCPSWD is not null and consists of one to seven digits, a user cannot invoke any local options without first entering the PROCPSWD value on the Craft Access Code Entry screen.

*** Note:**

If the password length is shorter than the minimum length of four digits, the system changes the password to the default password.

⚠ Caution:

If you administer PROCPSWD as part of DHCP/HTTP administration, the value is stored and transmitted unencrypted. Therefore, PROCPSWD is not a high-security technique to inhibit a sophisticated user from getting access to local procedures unless you administer the parameter using page 3 of the system-parameters IP-options form in Communication Manager Release 4.0.

If you administer this password, you cannot gain access to all local procedures, including VIEW. VIEW is a read-only Craft option, using which you can review the current phone settings.

*** Note:**

The following table lists the parameters that are described are:

ALWCLRNOTIFY	NORTELAUTH	NVIKECONFIGMODE
NVIKEDHGRP	NVIKEID	NVIKEIDTYPE
NVIKEOVERTCP	NVIKEP1AUTHALG	NVIKEP1LIFESec
NVIKEP2AUTHALG	NVIKEP2ENCALG	NVIKEP2LIFESec
NVIKEPSK	NVIKEXCHGMODE	NVIPSECSUBNET
NVPFSDHGRP	NVSGIP	NVVPNAUTHTYPE
NVVPNCFGPROF	NVVPNCOPYTOS	NVVPNENCAPS
NVVPNMODE	NVVPNPSWD	NVVPNPSWDTYPE
NVVPNSVENDOR	NVVPNUSER	NVVPNUSERTYPE
NVXAUTH	VPNACTIVE	VPNALLOWTAGS
VPNCODE	VPNPROC	VPNTTS

! Important:

Avaya does not support IPv6 for the general market, and makes the software available to a specific set of customers with known limitations. Any additional limitation or bugs discovered within this release will be considered for resolution in future major releases.

H.323 customizable system parameters

This table lists the parameters that you can customize in the `46xxsettings.txt` file, their default values, parameter descriptions, and valid values.

Soft persistent parameters

Soft persistent parameters reset to the default values after reboot. When the phone tries to access the file server, the value of the parameter might be updated depending on the following conditions.

- If the file server is not accessible, the phone uses the stored persistent value.
- If either of the following conditions is true, the phone uses the default value:
 - The file server is accessible, but the `46xxsettings.txt` file is not available on the server.
 - The file server is accessible and the `46xxsettings.txt` file is downloaded to the phone, but the corresponding parameter is not present in the file.
- If the parameter is present in the downloaded `46xxsettings.txt` file, the phone uses the parameter value specified in the file.


Parameter name	Default value	Description and value range
ACOUSTIC_EXPOSURE_PROTECT_MODE_DEFAULT	1	<p>Specifies the default setting of the long-term acoustic exposure protection mode. Valid values are:</p> <ul style="list-style-type: none"> • 1: Long term acoustic protection mode is turned off. • 2: Long term acoustic protection mode is turned on. The default duration is set to dynamic. • 3: Long term acoustic protection mode is turned on. The default duration is set to 4 hours. • 4: Long term acoustic protection mode is turned on. The default duration is set to 8 hours.
ADMIN_HSEQUAL	1	<p>Handset Equalization alternative permission flag. Valid values are:</p> <ul style="list-style-type: none"> • 1: Use handset equalization that is optimized for acoustic TIA 810/920 performance. • 2: Use handset equalization that is optimized for electrical FCC Part 68 HAC telecoil performance. <p> Note:</p> <p>This parameter will only have an effect on a phone if the handset equalization has not been set by the user or by the HSEQUAL local procedure.</p>

Table continues...




Parameter name	Default value	Description and value range
AGCHAND	1	<p>Automatic Gain Control status for handset, 0=disabled, 1=enabled.</p> <p> Note:</p> <p>This parameter applies only if the user has not changed the Automatic Gain Control from the deskphone menu. The changes made by the user are stored in the backup/restore file as OPTAGCHAND, if BRURI has a valid value. The value of the OPTAGCHAND parameter in the backup/restore file takes precedence over the AGCHAND parameter. User can use the Clear operation to reset the configuration.</p>
AGCHEAD	1	<p>Automatic Gain Control status for headset, 0=disabled, 1=enabled.</p> <p> Note:</p> <p>This parameter applies only if the user has not changed the Automatic Gain Control from the deskphone menu. The changes made by the user are stored in the backup/restore file as OPTAGCHEAD, if BRURI has a valid value. The value of the OPTAGCHEAD parameter in the backup/restore file takes precedence over the AGCHEAD parameter. User can use the Clear operation to reset the configuration.</p>
AGCSPKR	1	<p>Automatic Gain Control status for Speaker, 0=disabled, 1=enabled.</p> <p> Note:</p> <p>This parameter applies only if the user has not changed the Automatic Gain Control from the deskphone menu. The changes made by the user are stored in the backup/restore file as OPTAGCSPKR, if BRURI has a valid value. The value of the OPTAGCSPKR parameter in the backup/restore file takes precedence over the AGCSPKR parameter. User can use the Clear operation to reset the configuration.</p>
AGENTGREETINGSDELAY	700	<p>Valid values: 0 – 3000</p> <p>where the value specifies the delay time (milli seconds) between call autoanswer and playing of an agent greeting.</p>

Table continues...

Parameter name	Default value	Description and value range
AGTACTIVESK	0	<p>Used to control the softkeys that are available to the agent on the deskphone. Valid values are:</p> <ul style="list-style-type: none"> • 0: Transfer softkey is available on the second row of softkeys, and Release on the first row. • 1: Release softkey is available on second row of softkeys, and Transfer on the first row. • 2: Release softkey is not available on first/second row of softkeys, because there can be more softkeys with value 2 other than mentioned. • 3: on an active call, the soft keys are labeled from left to right: Hold, Conf, Transfer, Drop in a non-call center environment.
AGTCALLINFOSTAT	1	<p>For Avaya Call Center use only.</p> <p>Automatically invokes Call-info permission when the caller-information button, (buttonType = 141), is administered on the deskphone and AGTCALLINFOSTAT has a value of 1. The deskphone transmits a virtual press of that button to the call server.</p> <p>The call server is expected to respond with a call-associated display message with possible content in Line 2. The Line 2 content, if any, is checked by the call server to see if it contains any strings specified by GREETINGDATAx when the corresponding GREETINGTYPEx begins with 4. The first such greeting with a match as specified in the Match Criteria is played.</p> <p>1 ASCII numeric digit. Valid values are:</p> <ul style="list-style-type: none"> • 0: Do not automatically invoke Call-info permission. • 1: Invoke the caller information permission to locate a greeting.
AGTCAINFOLINE	1	<p>Controls presentation of call associated information in the agent information line when the phone is in half width screen mode. Valid values are:</p> <ul style="list-style-type: none"> • 0: The Agent Information Line presents agent-oriented information only. • 1: The Agent Information Line presents agent-oriented information and call associated information.

Table continues...


Parameter name	Default value	Description and value range
AGTFWDBTNSTAT	1	For Avaya Call Center use only. Disables the Forward button permission flag. When the CALLCTRSTAT parameter has a value of 1 and AGTFWDBTNSTAT has a value of 1 and the deskphone has an application button labeled Forward, the deskphone generates an error beep and performs no forwarding action when the Forward button is pressed. 1 ASCII numeric digit. Valid values are: <ul style="list-style-type: none"> • 0: Do not disable the Forward button. • 1: Disable the Forward button.
AGTGREETINGSTAT	1	For Avaya Call Center use only. Indicates agent Greeting permission and determines whether the deskphone displays the Greeting softkey when the deskphone receives an incoming call. 1 ASCII numeric digit. Valid values are: <ul style="list-style-type: none"> • 0: Do not display the Greeting softkey upon alerting. • 1: Display the Greeting softkey upon alerting.
AGTVUSTATID  Note: AGTVUSTATID was previously known as AGTIDVUSTAT.	0	For Avaya Call Center user only. Specifies the VuStats format number for deriving call center Agent ID. Valid values are 1 or 2 ASCII numeric digits, 0 through 50.
AGTLOGINFAC	#94	For Avaya Call Center use only. Indicates the Feature Access Code agents use to sign in to the call center. Valid values are 1 to 4 ASCII dialable characters 0 through 9 plus star (*) and pound (#).
AGTLOGOUTFAC	#95	For Avaya Call Center use only. Specifies the Feature Access Code agents use to log out. Valid values are 1 to 4 dialable characters 0 through 9 plus star (*) and pound (#).

Table continues...

Parameter name	Default value	Description and value range
AGTSPKRSTAT	1	<p>For Avaya Call Center use only. Disables or enables the speakerphone permission flag. 1 ASCII numeric digit. Valid values are:</p> <ul style="list-style-type: none"> • 0: Normal speaker operation; agent can activate or deactivate the Speakerphone. • 1: Speaker is disabled; agent cannot activate or deactivate the Speakerphone provided (CALLCTRSTAT=1 & non-null Agent ID). • 2: If the deskphone is a 9641G, and other conditions are met (CALLCTRSTAT=1 & Release button is administered & non-null Agent ID), then the Speaker button acts as a Release button. • 2: If the deskphone is NOT a 9641G, and if (CALLCTRSTAT=1 & non-null Agent ID), then the Speaker button is disabled. • 3: If (CALLCTRSTAT=1 & Release button is administered & non-null Agent ID), then the Speaker button acts as a Release button. • 4: If the Release button is administered, then the Speaker button acts as a Release button irrespective of whether the Agent is logged in or not.
AGTTIMESTAT	1	<p>For Avaya Call Center use only. Suppresses the date/time permission flag and display on the Title line. 1 ASCII numeric digit. Valid values are:</p> <ul style="list-style-type: none"> • 0: Display the date and time on the top display line. • 1: Do not display date and time on the top display line.
AGTTRANSLTO	to	<p>For Avaya Call Center use only. A text string used along with other user-set text strings and translation parameters AGTTRANSLCLBK, AGTTRANSLPRI, AGTTRANSLPK, and AGTTRANSLICOM to parse a call-associated display message when a call appearance is in the Alerting call state. The Agent Information line displays the result and provides information about the incoming call. 1 to 6 UTF-8 characters.</p>
AGTTRANSLCLBK	callback	<p>For Avaya Call Center use only. A text string used along with other user-set text strings and translation parameters AGTTRANSLTO, AGTTRANSLPRI, AGTTRANSLPK, and AGTTRANSLICOM to parse a call-associated display message when a call appearance is in the Alerting call state. The result displays on the Agent Information line and provides information about the incoming call. 1 to 6 UTF-8 characters.</p>

Table continues...

Parameter name	Default value	Description and value range
AGTTRANSLPRI	priority	For Avaya Call Center use only. A text string used along with other user-set text strings and translation parameters AGTTRANSLTO, AGTTRANSLCLBK, AGTTRANSLPK, and AGTTRANSLICOM to parse a call-associated display message when a call appearance is in the Alerting call state. The result displays on the Agent Information line and provides information about the incoming call. 1 to 6 UTF-8 characters.
AGTTRANSLPK	park	For Avaya Call Center use only. A text string used along with other user-set text strings and translation parameters AGTTRANSLTO, AGTTRANSLCLBK, AGTTRANSLPRI, and AGTTRANSLICOM to parse a call-associated display message when a call appearance is in the Alerting call state. The result displays on the Agent Information line and provides information about the incoming call. 1 to 6 UTF-8 characters.
AGTTRANSLICOM	ICOM	For Avaya Call Center use only. A text string used along with other user-set text strings and translation parameters AGTTRANSLTO, AGTTRANSLCLBK, AGTTRANSLPRI, and AGTTRANSLPK to parse a call-associated display message when a call appearance is in the Alerting call state. The result displays on the Agent Information line and provides information about the incoming call. 1 to 6 UTF-8 characters.
AMADMIN	Null	WML-Application URI. The URI used to obtain the AvayaMenuAdmin.txt file for WML-applications under the A (AVAYA) Menu. Specify the HTTP server and directory path to the administration file. Do not specify the administration file name.
APPNAME	Null	The file name of the Signed Application or Library Software Package that the deskphone downloads and installs during power-up or reset if it has not already been downloaded and installed. You should set this parameter only in an upgrade file.
APPSTAT	1	Controls whether specific applications are enabled, restricted, or disabled. Values are: <ul style="list-style-type: none"> • 0: Speed DialCall Log, and Redial disabled. • 1: all applications enabled • 2: Speed Dial (Contacts) changes and Call Log disabled and Redial last number only. • 3: Speed Dial (Contacts) changes disabled, (Contacts) changes.

Table continues...

Parameter name	Default value	Description and value range
APPLICATIONWD	1	Controls whether the application watchdog is enabled 1 or disabled 0. The application watchdog is a software process that, if enabled, monitors other software processes to determine whether the processes have become unresponsive, at which point it generates a log event and either kills the process or resets the deskphone.
AUDASYS	3	Globally controls audible alerting. Possible system settings for audible alerting are 0 through 3 as follows: <ul style="list-style-type: none"> • 0: Audible Alerting is Off; user cannot change this setting. The volume level of the ringer cannot be changed and will remain 0 even if the backup file restored includes a volume level for ringer larger than 0. • 1: Audible Alerting is On; user cannot change this setting. The volume level of the ringer cannot be set to 0 even if the backup file restored includes a volume level for ringer equal to 0 (in this case the default volume level 5 will be used). • 2: Audible Alerting is Off; user can change this setting. • 3: Audible Alerting is On; user can change this setting.
AUDIOENV	0	Audio environment selection index. Valid values are 0 through 299. Note that pre-Release 2.0 software has different valid ranges.
AUDIOSTHD	0	Headset sidetone setting. Valid values for applicable sidetone masking ratings (STMR) are: <ul style="list-style-type: none"> • 0: nominal STMR, no change to sidetone level. • 1: nominal +9 STMR, three steps softer than nominal. • 2: nominal +21 STMR (off), no sidetone (inaudible). • 3: nominal +3 STMR, one level softer than nominal. • 4: nominal +6 STMR, two steps softer than nominal. • 5: nominal +12 STMR, four steps softer than nominal. • 6: nominal +15 STMR, five steps softer than nominal. • 7: nominal +18 STMR, six steps softer than nominal. • 8: nominal -3 STMR, one step louder than nominal. • 9: nominal -6 STMR, two steps louder than nominal. Pre-Release 6.2 software has different valid ranges. For more information on fine-tuning your IP phones, see <i>Audio Quality Tuning for IP Telephones</i> , 100054528 on the Avaya Support site at www.avaya.com/support .

Table continues...

Parameter name	Default value	Description and value range
AUDIOSTHS	0	<p>Handset sidetone setting. Valid values are:</p> <ul style="list-style-type: none"> • 0: nominal STMR, no change to sidetone level. • 1: nominal +9 STMR, three steps softer than nominal. • 2: nominal +21 STMR (off), no sidetone (inaudible). • 3: nominal +3 STMR, one level softer than nominal. • 4: nominal +6 STMR, two steps softer than nominal. • 5: nominal +12 STMR, four steps softer than nominal. • 6: nominal +15 STMR, five steps softer than nominal. • 7: nominal +18 STMR, six steps softer than nominal. • 8: nominal -3 STMR, one step louder than nominal. • 9: nominal -6 STMR, two steps louder than nominal. <p>Pre-Release 6.2 software has different valid ranges.</p> <p>For more information on fine-tuning your IP phones, see <i>Audio Quality Tuning for IP Telephones</i>, 100054528 on the Avaya Support site at www.avaya.com/support.</p>
AUTH	0	Script file authentication value (0=HTTP is acceptable, 1=HTTPS is required).
BAKLIGHTOFF	120	Number of minutes without display activity to wait before setting the backlight to its lowest level. The default is 120 minutes (2 hours). Valid values range from zero to 999 minutes (16.65 hours).
BLUETOOTHSTAT	1	<p>Bluetooth permission flag:</p> <ul style="list-style-type: none"> • 0: Bluetooth is disabled. • 1: Bluetooth is enabled. <p>When Bluetooth is disabled through BLUETOOTHSTAT, the user cannot override this setting locally on the deskphone.</p>

Table continues...

Parameter name	Default value	Description and value range
BRAUTH	0	<p>Backup/restore authentication control. Valid values are:</p> <ul style="list-style-type: none"> • 0: The IP address of the call server and registration password of the deskphone is not included as part of GET or PUT Authorization header, or no digital certificate has been downloaded. • 1: If at least one digital certificate is downloaded based on TRUSTCERTS. The IP address of the call server with which the deskphone is registered and the registration password of the deskphone are included as the credentials in an Authorization request-header in each transmitted GET and PUT method if and only if the value of BRAUTH is 1.
BRURI	Null	<p>URI used for HTTP backup and retrieval of user data. Specify HTTP server and directory path to backup file. Do not specify backup file name. Value: 0-255 ASCII characters.</p> <p>96x0 H.323 R3.2/96x1 H.323 R6.0 phones support in addition a format of http://username:password@... or https://username:password@... for HTTP Basic authentication. The username and password are removed from the configured URI and used in the authorization header. The HTTP request will be sent to the URI without the username and password fields.</p> <p>For example:</p> <p>SET BRURI http://Administrator:Catt*123@10.10.10.6/Backup/</p> <p>SET BRURI http://ipphone:Avaya1234@10.10.10.1</p>

Table continues...


Parameter name	Default value	Description and value range
CADISPMODE	0	<p>Specifies whether to keep the display of the call appearance label in the call state idle mode or not, and whether to add prefix or suffix to identify the bridge or line number. The parameter is supported with Avaya Communication Manager only. Valid values are:</p> <ul style="list-style-type: none"> • 0: Labels are changed according to call state where Avaya Communication Manager provides the labels. • 1: The idle call label is presented independent on call states. In addition, "a." to "z." lowercase, and then "A." to "Z." uppercase are added as prefix in full width screen or as a suffix on the right column and a prefix on the left column in half width screen. "a." to "z." are added to bridged and line appearances according to the bridged or line button order. • 2: The idle call label is presented independent on call states as in 1, but without addition of "a." to "z." lowercase (and then "A."-"Z.") strings. If personalized label is configured for line/bridged appearance then it will be used instead of the idle call label assigned by the Communication Manager.
CALCSTAT	1	<p>Applies only to deskphones running software Release 6.0 and later. Specifies whether the Calculator application must be displayed or enabled. Valid values are:</p> <ul style="list-style-type: none"> • 0: No, disable the Calculator application. • 1: Yes, enable the Calculator application.
CALLCTRSTAT	0	<p>Applicable only to Call Centers. Call Center functionality flag. 1 ASCII numeric digit. Valid values are:</p> <ul style="list-style-type: none"> • 0: Call Center functionality does not apply; do not provide access to call center options/functions. • 1: Call Center functionality applies; allow agent access to call center functions like greetings and data backup. <p> Note:</p> <p>This parameter is soft persistent.</p>

Table continues...

Parameter name	Default value	Description and value range
CALLAPPRSELMODE	0	Controls highlighting of a call appearance during an incoming call. This parameter is applicable only if the deskphone is registered to Communication Manager. Valid values are: <ul style="list-style-type: none"> • 0: The call appearance of the incoming call is highlighted. The softkeys for the incoming call are displayed. For example, Answer or Ignore, if no other call is active; Ans Hold, Ans Drop, or Ignore, if a call is active. • 1: The highlight of the call appearance is on the active call or call on hold. The softkeys for the hold call are displayed, and not for the incoming call.
CALL_LOG_JOURNAL	0	Valid values are 0 or 1. Value of 1 triggers restore of call log journal.
CLBACKUPTIME	15	Specifies the minimum interval, in minutes, between backups of the Call Log, if the values of LOGBACKUP and CLBACKUPTIMESTAT are both 1. Valid values are 1 through 60.
CLBACKUPTIMESTAT	0	Specifies whether Call Log entries will be backed up only after a minimum interval as specified by the value of CLBACKUPTIME. This parameter only has an effect if the value of LOGBACKUP is 1. Valid values are: <ul style="list-style-type: none"> • 0: Call Log entries will be backed up as they are created. • 1: Call Log entries will be backed up after the interval specified by CLBACKUPTIME.
CCBTNSTAT	0	Specifies whether the values of CONFSTAT, DROPSTAT, HEADSTAT, HOLDSTAT, HOOKSTAT, MUTESTAT, and XFERSTAT are used to enabling and disabling the buttons associated with those parameters. Valid values are: <ul style="list-style-type: none"> • 0: The deskphone uses the values of these parameters. • 1: The deskphone ignores the values those parameters.

Table continues...


Parameter name	Default value	Description and value range
CCLOGOUTIDLESTAT	0	<p>Specifies whether an agent logging out of a call center will set the Headset LED and audio path to Off, or will leave the Headset LED and audio path On. Valid values are:</p> <ul style="list-style-type: none"> • 0: The deskphone automatically turns the headset LED Off and considers the audio and call states to be Idle. • 1: The deskphone does not turn the headset LED Off (if it is On) but still considers the audio and call states to be Idle. If the user is on a call at logout, the deskphone waits for the Disconnect message from the far end. <p> Note:</p> <p>When CCLOGOUTIDLESTAT = 1, the agent must answer the first call after reboot manually. After the first call the phone returns to headset off-hook idle state.</p>
CLDELCALLBK	0	<p>Call Log Delete Callback Flag. Deletes calls from the Missed Call Log when the user returns the call from the Call Log. Values are:</p> <ul style="list-style-type: none"> • 0: Yes. • 1: No.
CLDISPCONTENT	1	<p>Applies only to deskphones running software Release 6.0 and later. Call Log Display Content control; indicates whether call History list includes the caller's number or not. It specifies whether the name, the number, or both will be displayed for Call Log entries. Valid values are:</p> <ul style="list-style-type: none"> • 0: Displays both caller name and number. • 1: Displays the caller name but not number. • 2: Displays only the caller number but not the name.
CLEAR_EXTPSWD_ON_LOGOUT	0	<p>Specifies whether the extension and password are not displayed on a logged out deskphone. Valid values are:</p> <ul style="list-style-type: none"> • 0: The extension and/or password are displayed depending upon other parameters. • 1: The extension and password are not displayed in all cases
CERT_WARNING_DAYS	60	<p>Specifies the number of days before the expiration of a certificate that a warning should first appear on the phone screen. Log and syslog messages are generated for expired certificates. The warning reappears every 7 days.</p> <p>Valid values are 0 to 99. The value 0 disables the warning.</p>

Table continues...

Parameter name	Default value	Description and value range
CONFSTAT	0	Specifies whether the conference button is enabled or disabled when CCBTNSTAT is 0. Valid values are: <ul style="list-style-type: none"> • 0: The Conference button is disabled when CCBTNSTAT is 0. • 1: The Conference button is enabled.
CTASTAT	2	Call Type analysis status. Controls whether call type analysis algorithm in the Avaya Aura [®] Communication Manager is used during certain dialing behaviors. <ul style="list-style-type: none"> • 0: History, Redial, WML Browser, and Contacts do not use smart enbloc even if smart enbloc is enabled or supported by Avaya Aura[®] Communication Manager. • 1: Use smart enbloc if smart enbloc is enabled/ supported by Avaya Aura[®] Communication Manager by History, Redial and WML browser, but not for Contacts. • 2: Use smart enbloc if smart enbloc is enabled/ supported by Avaya Aura[®] Communication Manager by History, Redial and WML browser, but not for Contacts (Default).
DEFAULTRING	9	DEFAULTRING specifies the default ring tone. Valid values are 1 through 14.
DHCPPREF	6	Applies only to deskphones running software Release 6.0 and later. Specifies whether new values received via DHCPv4 or DHCPv6 are preferred when both are used. Valid values are: <ul style="list-style-type: none"> • 4: DHCPv4 is preferred. • 6: DHCPv6 is preferred.
DHCPSTVR	Null	Specifies DHCP server address(es). Format is dotted decimal or DNS format, separated by commas, with no spaces. Zero to 255 ASCII characters, including commas.
DHCPSTD	0	DHCP Standard lease violation flag. Indicates whether to keep the IP address if there is no response to lease renewal. If set to: <ul style="list-style-type: none"> • 0: (Yes) the deskphone continues using the IP address until it detects reset or a conflict. • 1: (No) the deskphone strictly follows the DHCP standard with respect to giving up IP addresses when the DHCP lease expires.
DIALFEATURES	Null	A list of feature number identifiers for softkey features available in the Dialing call state, for example, Redial. Zero to 255 ASCII characters consisting of 0 to 5 whole numbers separated by commas without any spaces.

Table continues...

Parameter name	Default value	Description and value range
DNSSRV	0.0.0.0	Text string containing the IP address of zero or more DNS servers, in dotted-decimal format, separated by commas with no intervening spaces, 0-255 ASCII characters, including commas.
DOMAIN	Null	Text string containing the domain name to be used when DNS names in parameter values are resolved into IP addresses. Valid values are 0-255 ASCII characters. If Null, do not leave spaces.
DOT1X	0	802.1X Supplicant operation mode. Valid values are: <ul style="list-style-type: none"> • 0: With PAE pass-through. • 1: with PAE pass-through and proxy Logoff. • 2: without PAE pass-through or proxy Logoff.
DOT1XEAPS	MD5	Specifies the EAP method used for 802.1X operation. Valid values are <i>MD5</i> and <i>TLS</i> .
DOT1XSTAT	0	Determines how the phone handles Supplicants. Valid values are: <ul style="list-style-type: none"> • 0: Supplicant operation is completely disabled. • 1: Supplicant operation is enabled, but responds only to received unicast EAPOL messages. • 2: Supplicant operation is enabled and responds to received unicast and multicast EAPOL messages.
DOT1XWAIT	0	Specifies whether the phone will wait for 802.1X authentication to complete before proceeding with DHCP operation. Valid values: <ul style="list-style-type: none"> • 0: Phone does not wait for 802.1X authentication to complete and continues DHCP operation. • 1: Phone waits for 802.1X authentication to complete to continue DHCP operation. • 2: Phone does not wait for a successful 802.1X authentication. Phone continues with DHCP operation disregarding 802.1x authentication status.

Table continues...

Parameter name	Default value	Description and value range
DOT1XEAPTLSONLYWITHCERT	1	<p>Specifies that 802.1x EAP-TLS is activated when there is an identity certificate installed.</p> <ul style="list-style-type: none"> 0: 802.1x EAP-TLS is activated immediately when DOT1XSTAT is set to 1 or 2 and the value of DOT1XEAPS is TLS. 1: 802.1x EAP-TLS is activated when DOT1XSTAT is set to 1 or 2 and the value of DOT1XEAPS is TLS. In addition, there must be an identity certificate and a minimum of one trusted certificate is installed.
DROPCLEAR	1	<p>VPN only. Specifies how clear IPsec packets are processed. One ASCII numeric digit. Valid values are:</p> <ul style="list-style-type: none"> 0: all other packets will be processed, but not by IPsec. 1: all other packets will be discarded.
DROPSTAT	0	<p>Specifies whether the Drop button is enabled or disabled when CCBTNSTAT is 0. Valid values are:</p> <ul style="list-style-type: none"> 0: The Drop button is disabled when CCBTNSTAT is 0. 1: The Drop button is enabled.
ENHDIALSTAT	1	<p>Specifies the dialing algorithm status. Controls whether algorithm defined by parameters is used during certain dialing behaviors. Valid values are:</p> <ul style="list-style-type: none"> 0: Disables algorithm. 1: Enables algorithm, but not for Contacts. 2: Enables algorithm, including Contacts. <p>If set to 1, the Administering dialing methods feature is on for all associated applications.</p>
FIPS_ENABLED	0	<p>Allows only FIPS 140-2 Level 1 validated cryptographic algorithms. To enable the JITC mode, set the value to 1.</p>
GRATARP	0	<p>Gratuitous ARP flag. Controls whether the deskphone processes gratuitous ARPS or ignores them.</p> <p>If you use Processor Ethernet (PE) duplication and if your phones are on the same subnet as the PE interfaces, set this parameter to 1, to allow the fastest failover to the new PE interface.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> 0: No, ignore gratuitous ARPS 1: Yes, process gratuitous ARPS

Table continues...

Parameter name	Default value	Description and value range
GRATNAV6	0	Applies only to deskphones running software Release 6.0 and later. Specifies whether the call server will process gratuitous and unsolicited IPv6 Neighbor Advertisement messages. A received message is considered unsolicited if the deskphone did not send a corresponding Neighbor Solicitation message first; it is not determined by the value of the Solicited flag in the received message. An IPv6 unsolicited Neighbor Advertisement message is similar to a gratuitous ARP message in IPv4.
GUESTDURATION	2	Guest login duration in hours. One or two ASCII numeric digits. Valid values are 1, through 12.
GUESTLOGINSTAT	0	Guest login permission flag. If set to 1, the Guest Login option is listed on the Avaya Menu; if set to 0, the Guest Login option is not available.
GUESTWARNING	5	Guest login warning in minutes to indicate when to notify the user that <i>GUESTLOGIN</i> will expire. One or two ASCII numeric digits. Valid values are 1 through 15.
HEADSYS	0 if CALLCTRSTAT = 0, else 1	Headset operational mode. Specifies whether the deskphone will go on-hook if the headset is active when a Disconnect message is received. One ASCII numeric digit. Valid values are: <ul style="list-style-type: none"> • 0 or 2: The deskphone will go on-hook if a Disconnect message is received when the headset is active. • 1 or 3: Enabled, Disconnect messages are ignored when the headset is active.
HEADSTAT	0	Specifies whether the Headset button is enabled or disabled when CCBTNSTAT is 0. The value is ignored by the deskphones that do not have a Headset button. Valid values are: <ul style="list-style-type: none"> • 0: The Headset button is disabled when CCBTNSTAT is 0. • 1: The Headset button is enabled.

Table continues...


Parameter name	Default value	Description and value range
HEADSETBIDIR	0	<p>Specifies the permission flag for enabling or disabling the Headset Bi-directional functionality. Valid values are:</p> <ul style="list-style-type: none"> • 0: Default, Bi-directional functionality disabled. • 1: Switchhook and Alerting. • 2: Switchhook only. <p> Note:</p> <p>This parameter applies only if the user has not changed the Call Settings from the deskphone menu. The changes made by the user are stored in the backup/restore file. User can use the Clear operation to reset the configuration.</p>
HEADSET_PROFILE_DEFAULT	1	Specifies the number of the default headset audio profile. Values: 1 to 20.
HEADSET_PROFILE_NAMES	Null	<p>Specifies an ordered list of names to be displayed for headset audio profile selection. Value: 0 to 255 UTF-8 characters.</p> <ul style="list-style-type: none"> • Names are separated by commas without any intervening spaces. • Two commas in succession indicate a null name, which means that the default name is displayed for the corresponding profile. • Names may contain spaces but entire name must be in quotes. <p>For example: SET HEADSET_PROFILE_NAMES "Acme Earwigs,,Spinco Ear Horns"</p>
HOLDSTAT	0	<p>Specifies whether the Hold button is enabled or disabled when CCBTNSTAT is 0. Valid values are:</p> <ul style="list-style-type: none"> • 0: The Hold button is disabled when CCBTNSTAT is 0. • 1: The Hold button is enabled.
HOOKSTAT	0	<p>Specifies whether the switchhook is enabled or disabled when CCBTNSTAT is 0. Valid values are:</p> <ul style="list-style-type: none"> • 0: The switchhook is disabled when CCBTNSTAT is 0. • 1: The switchhook is enabled.

Table continues...


Parameter name	Default value	Description and value range
HTTPDIR	Null	HTTP server directory path. The path name prepended to all file names used in HTTP <i>GET</i> operations during initialization. Value: 0-127 ASCII characters, no spaces. Null is a valid value. Leading or trailing slashes are not required. The command syntax is <i>SET HTTPDIR myhttpdir</i> where <i>myhttpdir</i> is your HTTP server path. HTTPDIR is the path for all HTTP operations except for BRURI.
HTTPPORT	80	TCP port number used for HTTP file downloading. 2 to 5 ASCII numeric digits. Valid values are 80 through 65535. Note that when the file server is on Communication Manager, set this value to 81 that is the port required for HTTP downloads rather than the using the default.
HTTPSRVR	Null	IP address(es) or DNS Name(s) of HTTP file servers used to download deskphone files. Dotted decimal or DNS format, separated by commas, 0-255 ASCII characters, including commas.
H323SIGPROTOCOL	0	Specifies the signaling protocol that the phone will send in the Gatekeeper Request. <ul style="list-style-type: none"> • 0: TLS, Annex-H or challenge authentication (default). • 1: TLS, Annex-H. • 2: TLS authentication.
ICMPDU	0	Controls whether ICMP Destination Unreachable messages will be processed. Values are: 0=No, 1=Send limited Port Unreachable messages, 2=Send Protocol and Port Unreachable messages.
ICMPRED	0	Controls whether ICMP Redirect messages will be processed. Values are: <ul style="list-style-type: none"> • 0: No. • 1: Yes.
IDLEFEATURES	Null	A list of feature number identifiers for softkey features potentially available in the Idle call state, for example, Redial. Zero to 255 ASCII characters consisting of zero to six whole numbers separated by commas without any intervening spaces. <p> Note:</p> <p>H.323 Release 6.4 onwards, information of the parameter is saved in a non-volatile memor, thus retaining the information even after power down or reboot.</p>

Table continues...

Parameter name	Default value	Description and value range
IGNORESTAT	1	<p>Specifies whether the Ignore button is enabled or disabled. The IGNORESTAT parameter can be used in call center and non call center environments.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • 0: The Ignore button is disabled when CCBTNSTAT is 0 • 1: The Ignore button is enabled (default) <p>For example: SET IGNORESTAT 1</p> <p>* Note:</p> <p>The HOLDSTAT, CONFSTAT, and other parameters can be used only in call center environment.</p>
IPPREF	6	<p>Applies only to deskphones running software Release 6.0 and later. Specifies which type of IP address (IPv4 or IPv6) will be tried first if DNS returns both types. Valid values are:</p> <ul style="list-style-type: none"> • 4: Try IPv4 addresses first over DHCPv6 if DNS returns both types. • 6: Try IPv6 addresses first over DHCPv4 if DNS returns both types.
IPV6STAT	0	<p>Applies only to deskphones running software Release 6.0 and later. Specifies whether IPv6 will be enabled. Valid values are:</p> <ul style="list-style-type: none"> • 0: IPv6 is disabled. • 1: IPv6 is supported/enabled. <p>* Note:</p> <p>Avaya does not support IPv6 for the general market, and makes the software available to a specific set of customers with known limitations. Any additional limitation or bugs discovered within this release will be considered for resolution in future major releases.</p>
L2Q	0	<p>Controls whether Layer 2 frames have IEEE 802.1Q tags:</p> <ul style="list-style-type: none"> • 0: auto. • 1: enabled. • 2: disabled.

Table continues...

Parameter name	Default value	Description and value range
L2QVLAN	0	<p>802.1Q VLAN Identifier (0 to 4094). Null (" ") is not a valid value and the value cannot contain spaces. VLAN identifier that IP deskphones use. Set this parameter only if IP deskphones use a VLAN that is separate from the default data VLAN.</p> <p>If you must configure the VLAN identifier using H.323 signaling based on Communication Manager administration forms, the VLAN should not be set here. From software Release 2.0, L2QVLAN will always be initialized from the corresponding system initialization value at power-up, but will not be initialized from the system initialization value after a reset.</p>
LANG0STAT	1	<p>Controls whether the built-in English language text strings can be selected by the user. Valid values are:</p> <ul style="list-style-type: none"> • 0: User cannot select English language text strings • 1: User can select English language text strings. <p>SET LANG0STAT 1</p>
LANGxFILE	Null	<p>Contains the name of the language file x, where x is 1 through 4. The file name must end in .txt. Example: SET LANG1FILE "mlf_russian.txt"</p> <ul style="list-style-type: none"> • LANG1FILE • LANG2FILE • LANG3FILE • LANG4FILE
LANGLARGEFONT	Null	<p>Larger text font file name. A string of up to 32 characters specifies the loadable language file on the HTTP server for the Large Text font.</p>

Table continues...

Parameter name	Default value	Description and value range
LANGSYS	Null	<p>System-wide language that contains the name of the default system language file, if any. Value is 0 to 32 ASCII characters. The file name must end in .txt. The default is a null string. Example: SET LANGSYS mlf_german.txt</p> <p>* Note:</p> <p>This parameter applies only if the user has not changed the Screen & Sound Options from the deskphone menu. The changes made by the user are stored in the backup/restore file as LANGUSER, if BRURI has a valid value. The value of the LANGUSER parameter in the backup/restore file takes precedence over the LANGSYS parameter. User can use the Clear operation to reset the configuration.</p>
LEDMODE	0	<p>Supports new LED behavior Valid values 0= Old behavior, and would mean that the red led is controlled locally by the phone, 1 = New behavior and would mean the buttons red LEDs are controlled by CM .</p> <p>Example: If new behavior is activated, Button module and phone LEDs are aligned and will change according to call state.</p>
LLDP_XMIT_SECS	30	<p>Specifies the rate in seconds at which LLDP messages will be transmitted.</p> <p>Valid values are 1 to 4 ASCII numeric digits, "1" through "3600"</p> <p>Main usage is for the SSO application to discover the phone faster.</p>
LOCALZIPTONEATT	35	<p>Controls the local phone ziptone volume when AUTOANSSTAT= 1 Note: If Auto answer is configured on the CM and not using the AUTOANSSTAT setting, this parameter does not influence that zip tone volume.</p> <p>Valid values: 0 - 95, where 0 = Loudest and 95 = Lowest.</p>
LOGBACKUP	1	<p>Indicates whether the call log of the user should be backed up. Values are:</p> <ul style="list-style-type: none"> • 0: No. • 1: Yes. The Call Log is backed up to the same backup file as all other user data subject to normal administration of that file.

Table continues...

Parameter name	Default value	Description and value range
LOGLOCAL	0	<p>Event Log Severity Level. Valid values are one 0-8 ASCII numeric digit. Controls the level of events logged in the endptRecentLog and endptResetLog objects in the SNMP MIB. Events with the selected level and with a higher severity level are logged. Valid values are:</p> <ul style="list-style-type: none"> • 0: disabled • 1: emergencies • 2: alerts • 3: critical • 4: errors • 5: warnings • 6: notices • 7: information • 8: debug
LOGMISSEDONCE	0	<p>Indicates that only one Call Log entry for multiple Missed calls from the same originating phone number must be maintained. Values are:</p> <ul style="list-style-type: none"> • 0: No; each Missed Call creates a new Call Log entry. • 1: Yes; each Missed Call Log entry is maintained, along with a Missed Call counter that tracks the number of times (up to 99) the originating number called.
LOGSRVR	Null	Syslog Server IP address. Zero or one IP address in dotted-decimal, colon-hex, or DNS Name format (0-15 ASCII characters).
LOGUNSEEN	0	<p>Indicates that a Call Log entry should be maintained for calls that are redirected from the deskphone, for example, Call forwarded calls. Values are:</p> <ul style="list-style-type: none"> • 0: No. • 1: Yes. <p>CM 5.2 or later is required for this feature to work.</p>
LOGTOFILE	0	<p>Specifies whether optional debug printf strings will be logged to an internal file.</p> <p>If LOGTOFILE:</p> <ul style="list-style-type: none"> • 0: not logged. • 1: optional debug printf strings are logged to an internal file.

Table continues...

Parameter name	Default value	Description and value range
MCIPADD	0.0.0.0	Call Server address. Zero or more Avaya Communication Manager server IP addresses. Format is dotted-decimal or DNS name format, separated by commas without intervening spaces (0-255 ASCII characters, including commas). Null is a valid value.
MSGNUM	Null	Voice mail system deskphone or extension number. Specifies the number to be dialed automatically when the deskphone user presses the Message button. MSGNUM is only used when the phone is aliased using non-native support. Messaging must be configured for native support. Value: 0-30 ASCII dialable characters are 0 through 9, star (*) and pound (#) and no spaces. Null is a valid value.
MUTESTAT	0	Specifies whether the Mute button is enabled or disabled when CCBTNSTAT is 0. Valid values are: <ul style="list-style-type: none"> • 0: The Mute button is disabled when CCBTNSTAT is 0. • 1: The Mute button is enabled.
MYCERTCAID	"CAIdentifier"	Certificate Authority Identifier to be used in a certificate request. 0 to 255 ASCII characters.
MYCERTCN	"\$SERIALNO"	Common Name of the Subject of a certificate request. 0 to 255 ASCII characters that contain the string \$SERIALNO or \$MACADDR.
MYCERTDN	Null	Additional information for the Subject of a certificate request. 0 to 255 ASCII characters.
MYCERTKEYLEN	1024	Bit length of the private key to be generated for a certificate request. 4 ASCII numeric digits, 1024 through 2048.
MYCERTKEYUSAGE	NULL	Specifies the purpose for which a certificate is issued. 0 to 255 ASCII characters. List of text strings, separated by commas without any intervening spaces, that is compared to the values specified for the X.509 KeyUsage extension. For each matching value, the corresponding bit will be set in the SCEP PKCSReq; invalid strings will be ignored; Possible values are: "digitalSignature", "nonRepudiation", "keyEncipherment", "dataEncipherment", "Agreement", "keyCertSign", "cRLSign", "encipherOnly", "decipherOnly".

Table continues...


Parameter name	Default value	Description and value range
MYCERTRENEW	90	<p>Specifies the percentage of the identity certificate's validity interval after which renewal procedure is initiated. Valid values are 1 or 2 ASCII numeric digits, 1 through 99.</p> <p> Note:</p> <p>Identity certificate renewal using SCEP is supported whether IPSec VPN tunnel is active or not.</p>
MYCERTURL	Null	URL to be used to contact an SCEP server. Zero to 255 ASCII characters, zero or one URL.
MYCERTWAIT	1	<p>Specifies whether the deskphone will wait until a pending certificate request is complete, or whether it will periodically check in the background. 1 ASCII numeric digit, 0 or 1 as follows:</p> <ul style="list-style-type: none"> • 0: SCEP will remain in progress until the request for a certificate is granted or rejected or until a response is received indicating that the request is pending for manual approval. • 1 : If a connection to the SCEP server is successfully established, SCEP will remain in progress until the request for a certificate is granted or rejected.
NDREDV6	0	<p>Applies only to deskphones running software Release 6.0 and later. Controls whether IPv6 Neighbor Discovery Redirect messages will be processed. Valid values are:</p> <ul style="list-style-type: none"> • 0: Ignore received Redirect messages. • 1: Process received Redirect messages.
NVHTTPSRVR	Null	<p>Applies to both VPN and non-VPN settings. NVHTTPSRVR is the HTTP file server IP addresses used to initialize HTTPSRVR the next time the phone starts up. Zero to 255 ASCII characters: zero or more IP addresses in dotted decimal, colon-hex, or DNS name format, separated by commas without any intervening spaces.</p> <p>NVHTTPSRVR is provided for VPN mode so that a file server IP address can be pre configured and saved in non-volatile memory. For more information, see <i>VPN Setup Guide for 9600 Series IP Telephones</i>, 16-602968.</p>
NVMCIPADD	Null	Call server IP addresses. Zero to 255 ASCII characters; zero or more IP addresses in dotted-decimal, colon-hex, or DNS name format, separated by commas without any intervening spaces.

Table continues...

Parameter name	Default value	Description and value range
NVTLSRVR	Null	VPN and non-VPN. HTTPS file server IP addresses used to initialize TLSRVR the next time the phone starts up. 0 to 255 ASCII characters: zero or more IP addresses in dotted decimal, colon-hex, or DNS name format, separated by commas without any intervening spaces. For more information, see <i>VPN Setup Guide for 9600 Series IP Telephones</i> , 16-602968.
OCSP_ACCEPT_UNK	1	Specifies whether a certificate is authenticated even if its revocation status cannot be determined. Valid values are: <ul style="list-style-type: none"> • 0: Certificate is considered to be revoked if the certificate revocation status is unknown. TLS connection is closed. • 1: Certificate revocation operation will accept certificates for which the certificate revocation is unknown.
OCSP_ENABLED	0	Specifies whether OCSP is used to verify the revocation status of the certificates. Valid values are: <ul style="list-style-type: none"> • 0: OCSP is not used. • 1: OCSP is used to check the revocation status for the certificates presented by peers for any TLS connection. For example, HTTPS, 802.1x with EAP-TLS, SLA Mon agent, IPsec VPN, or SSO.
OCSP_NONCE	1	Specifies whether a nonce is included in OCSP requests and expected in OCSP responses. Valid values are: 0 or 1.
OCSP_URI	Null	Specifies a URI for an OCSP responder. The URI can be an IP address or a host name.
OCSP_URI_PREF	1	OCSP responder URI can either be obtained from the certificate presented by the server, or can be locally configured on the phone in OCSP_URI. OCSP_URI_PREF specifies the preference between the two sources. Valid values are: <ul style="list-style-type: none"> • 1: OCSP_URI is used first and then the value from the OCSP field of the Authority Information Access (AIA) extension of the certificate is checked. • 2: OCSP field of the Authority Information Access (AIA) extension of the certificate is checked first and then OCSP_URI is used.

Table continues...

Parameter name	Default value	Description and value range
OCSP_TRUSTCERTS	Null	Specifies the list of the OCSP trusted certificates. This value is required if the OCSP responder uses a different CA for the server certificate than the root CA.
OPSTAT	111	Option status flag(s) (1 or 3 ASCII numeric digits) indicate which options are user-selectable. The default of 111 grants access to all options and related applications. Single digit valid values are: 1=user can access all options, including Logout, 2= user can access only view-oriented applications. Three-digit valid values are a concatenation of binary values, in the form <i>abc</i> , where each letter represents a 0 (disabled/off) or 1 (enabled/on), interpreted as: <i>a</i> = base settings for all user options and related applications, except as in <i>b</i> or <i>c</i> . <i>b</i> = setting for view-oriented applications (for example, the Network Information application), as applicable. <i>c</i> = setting for Logout application, if applicable. The binary 0 does not allow an end user to see or invoke options and related applications. Setting the flag to binary 1 gives full display and access to all options and related applications.
OPSTAT2	0	OPSTAT override flag. If set to 0, OPSTAT is not affected. If set to 1, OPSTAT is unaffected with the exception that any changes to customized labels in the backup file are uploaded and used as if OPSTAT permitted this action.
OPSTATCC	0	Specifies whether Call Center options such as Greetings will be presented to the user even if the value of OPSTAT is set to disable user options. Note that the value of CALLCTRSTAT must be 1 for OPSTATCC to be used. <ul style="list-style-type: none"> • 0: Call Center options will be displayed based on the value of OPSTAT (default). • 1: Call Center options will be displayed based on the value of OPSTATCC.
PHNCC	1	Telephone country code. The administered international country code for the location by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1-3 digits, from 1 to 999.
PHNDPLENGTH	5	Internal extension deskphone number length. Specifies the number of digits associated with internal extension numbers by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 or 2 digits, from 3 to 13.

Table continues...

Parameter name	Default value	Description and value range
PHNEMERGNUM	Null	Emergency deskphone/extension number. Specifies the number to be dialed automatically when the deskphone user presses the Emerg button. Value: 0-30 ASCII dialable characters from 0 through 9, star (*), pound (#) and no spaces. Null is a valid value.
PHNIC	011	Telephone international access code. The maximum number of digits, if any, dialed to access public network international trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 0-4 digits.
PHNLD	1	Telephone long distance access code. The digit, if any, dialed to access public network long distance trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 digit or " " (Null).
PHNLDLENGTH	10	Length of national deskphone number. The number of digits in the longest possible national deskphone number by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 1 or 2 digits, from "3" to "10." Range: 1 or 2 ASCII numeric characters, from 5 to 15.
PHNMUTEALERT_BLOCK	1	Specifies whether to allow or restrict the mute alerting feature for the end user. Valid values are: <ul style="list-style-type: none"> • 0: End user can use mute alerting. • 1: End user cannot use mute alerting.
PHNOL	9	Outside line access code. The character(s) dialed, including # and *, if any, to access public network local trunks by the algorithm that dials calls from the incoming Call Log or from Web pages. Range: 0-2 dialable characters, including " " (Null).
PHNSCRALL	0	Specifies whether the deskphone displays separate screens for Call Appearance and Feature buttons. <ul style="list-style-type: none"> • 0: Separate screens for Call Appearance and Feature buttons. • 1: Consolidated screen for Call Appearance and Feature buttons.

Table continues...


Parameter name	Default value	Description and value range
PHNSCRCOLUMNS	0	<p>Valid values are 0 or 1</p> <p>Specifies whether the Phone Screen is presented with one (full-width) or two (each half-width) columns.</p> <p> Note:</p> <p>The PHNSCRCOLUMNS is enforced only if the user does not change the value in the Phone Screen Width field. The user can change the settings on the phone screen, by changing the value of the Phone Screen Width field from the HOME > Options & Settings > Screen & Sound Options menu. The user changes are stored in backup/restore file as PHNSCRWIDTH.</p> <ul style="list-style-type: none"> • If BRURI has a valid value, the restored file that includes the PHNSCRWIDTH parameter will take precedence over PHNSCRCOLUMNS. • If BRURI is not valid, but the user still changes the value of the Phone Screen Width field, then user value will take precedence over PHNSCRCOLUMNS. <p>The CLEAR operation clears the user configuration.</p>
PHY1STAT	1	<p>Ethernet line interface setting:</p> <ul style="list-style-type: none"> • 1: auto-negotiate • 2: 10 Mbps half-duplex • 3: 10 Mbps full-duplex • 4: 100 Mbps half-duplex • 5: 100 Mbps full-duplex • 6: 1000 Mbps full-duplex, if supported by the hardware.
PHY2PRIO	0	<p>Layer 2 priority value for frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is 1 (enabled). Values are from 0 through 7 and correspond to the drop-down menu selection.</p>

Table continues...

Parameter name	Default value	Description and value range
PHY2STAT	1	<p>Secondary Ethernet interface setting:</p> <ul style="list-style-type: none"> • 0: Secondary Ethernet interface off/disabled • 1: auto-negotiate • 2: 10 Mbps half-duplex • 3: 10 Mbps full-duplex • 4: 100 Mbps half-duplex • 5: 100 Mbps full-duplex • 6: 1000 Mbps full-duplex if supported by the hardware
PHY2VLAN	0	<p>VLAN identifier used by frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is “1” (enabled).</p> <p>Value is 1-4 ASCII numeric digits from 0 to 4094. Null is not a valid value, nor can the value contain spaces. If this value is set by LLDP using the Port VLAN ID TLV value, the value will not change regardless of settings from other sources.</p>
PKCS12URL	Null	<p>Specifies the URL to download a PKCS #12 file containing an identity certificate and its private key.</p> <p>Value is a string that contains either of the following variables, along with other characters:</p> <ul style="list-style-type: none"> • \$SERIALNO: Is replaced by the serial number of the deskphone. • \$MACADDR: Is replaced by the MAC address of the deskphone. Must be specified without colons. For example, if Ethernet MAC address of a specific phone is 00-24-D7-E4-2E-98 and the PKCS12URL is <code>http://pkc12file_\$MACADDR.cer</code>, then the filename of the PKCS12 file for this phone on the file server will be <code>pkc12file_0024D7E42E98.cer</code>.
PINGREPLYV6	1	<p>Specifies whether ICMPv6 Echo Reply messages will be sent or not. Valid values are:</p> <ul style="list-style-type: none"> • 0: ICMPv6 Echo Reply messages will not be sent. • 1: ICMPv6 Echo Reply messages will be sent only in reply to received Echo Request messages with a Destination address equal to one of the deskphone's unicast IPv6 addresses. • 2: ICMPv6 Echo Reply messages will be sent in reply to received Echo Request messages with a Destination address equal to one of the unicast, multicast or anycast IPv6 addresses of the deskphone.

Table continues...

Parameter name	Default value	Description and value range
PROCPSWD	27238	Text string containing the local dial pad procedure password (Null or 1-7 ASCII digits). If set, password must be entered immediately after accessing the Craft Access Code Entry screen, either during initialization or when Mute or the Contacts button for the 9610 is pressed to access a craft procedure. Intended to facilitate restricted access to local procedures even when command sequences are known. Password is viewable, not hidden.
PROCSTAT	0	Local dial pad Administrative Options status (0=all Administrative (Craft) Options are allowed, 1=only VIEW is allowed).
PUSHCAP	2222	Push capabilities. Valid values are any three or four digit combination using only the digits 0, 1, or 2.
PUSHPORT	80	TCP listening port number used for the deskphone's HTTP server. 2 to 5 ASCII numeric digits, 80 through 65535.
QKLOGINSTAT	1	Quick login permission flag. Valid values are: <ul style="list-style-type: none"> • 0: Quick login not permitted; the user must explicitly enter the extension and password. • 1: Quick login permitted; user must press the pound (#) key to see the previous Extension and Password.
QLEVEL_MIN	4	Valid values are 1 to 6 Specifies the minimum quality level in which a low local network quality indication will not be displayed.
QTESTRESPONDER	Null	Specifies the IP address to which Qtest messages should be sent. The device at this address must support the echo service on UDP port 7, as specified in IETF RFC 862. Format is dotted decimal, colon-hex, or DNS format, separated by commas, with no spaces. Zero to 255 ASCII characters, including commas.
RECORDINGTONE	0	Recording tone permission flag: <ul style="list-style-type: none"> • 0: Recording tone is disabled. • 1: Recording tone is enabled. When recording tone is enabled, when the agent is on an active call or conference call, the deskphone inserts a tone into the audio stream every 15 seconds, so that both the user and the far end hears it. The recording tone has a frequency of 1400 Hz and a duration of 0.2 seconds.
RECORDINGTONE_INTER VAL	15	Recording tone interval. The number of seconds between recording tones, with a range from 1 to 60.

Table continues...

Parameter name	Default value	Description and value range
RECORDINGTONE_VOLUME	0	Volume of Recording tone played. (1 or 2 ASCII digits from '0' to '10'). The default plays the Recording tone at the same volume as the rest of the audio path; each higher number reduces the volume by 5 db.
REREGISTER	20	Registration timer in minutes. Controls an H.323 protocol timer that should only be changed under very special circumstances by someone who fully understands the system operation impact. Value is 1-120.
REUSETIME	60	The number of seconds to wait for successful completion of DHCP before reusing previous parameters on the default (port) VLAN. Valid values are 1 to 3 ASCII numeric digits, 0 and 20 through 999.
RFSNAME	Null	Applies only to deskphones running software Release 6.0 and later. The file name of the Signed Kernel/Root Software Package that should be downloaded and installed by the deskphone during power-up or reset if it has not already been downloaded and installed. This parameter should only be set in an upgrade file.
RINGBKFEATURES	Null	A list of feature number identifiers for softkey features potentially available in the active with far end ringback call state. Zero to 255 ASCII characters consisting of zero to three whole numbers separated by commas without any intervening spaces.
RINGTONESTYLE	0	The Ring Tone Style Menu initially offered to the user: <ul style="list-style-type: none"> • 0: Classic. • 1: Alternate, more modern ringtones.
RTCPMON	Null	Text string containing the 4-octet IP address of the RTCP monitor currently in use, in dotted decimal or DNS Name format (0-15 ASCII characters, no spaces).
SCEPPASSWORD	“\$SERIALNO”	Specifies a challenge password for SCEP. Zero to 50 ASCII characters.
SCEPBEFOREUPGRADE	0	When both SCEP and software upgrade are about to be done on the phone, this parameter specifies whether SCEP will be done before or after the software upgrade. <ul style="list-style-type: none"> • 0: SCEP will be done after software upgrade. • 1: SCEP will be done before software upgrade.

Table continues...

Parameter name	Default value	Description and value range
SCREENSAVER	Null	<p>Filename for a custom screen saver. 0 to 32 ASCII characters. Note that screen saver files must be in .jpg format.</p> <p>Acceptable characters for use in filenames are:</p> <ul style="list-style-type: none"> • 0 through 9 • A through Z • a through z • - (dash) • .(period) • _ (underscore)
SCREENSAVERON	240	<p>Number of idle time minutes after which the screen saver is turned on. The default is 240 minutes (4 hours). Valid values range from zero (disabled) to 999 minutes (16.65 hours). For 9670G phones, use HOMEIDLETIME instead.</p>
SERVER_CERT_RECHECK_HOURS	24	<p>Applicable for H.323 over TLS signaling only. Specifies the number of hours to verify the revocation status of the certificates that were used to establish a TLS connection.</p> <p>Valid values are 0 to 32767. The value 0 stops the verification.</p>
SLMCAP	0	<p>Specifies whether the SLA Monitor agent supports packet capture.</p> <p>Assign one of the following values:</p> <ul style="list-style-type: none"> • 0: Packet capture is disabled. • 1: Packet capture is enabled but without payloads. • 2: Packet capture is enabled with payloads. • 3: Packet capture is disabled. The feature is enabled from the CRAFT menu with payloads.
SLMCTRL	0	<p>Specifies whether the SLA Monitor agent supports device control.</p> <p>Assign one of the following values:</p> <ul style="list-style-type: none"> • 0: Device control is disabled. • 1: Device control is enabled. • 2: Device control is disabled. The feature is enabled from the CRAFT menu.
SLMPERF	0	<p>Valid values are 0 or 1.</p> <p>Specifies whether the SLA Monitor agent supports performance monitoring.</p>

Table continues...

Parameter name	Default value	Description and value range
SLMPORT	50011	Valid values are 6000 - 65535. Specifies the UDP port used to receive commands from the SLA Monitor server.
SLMSRVR	0.0.0.0:0	Specifies the source IP address and, optionally, the source port number of valid discovery messages from an SLA Monitor server.
SLMSTAT	0	0 or 1. Specifies whether the SLA Monitor agent will be enabled.
SSH_ALLOWED	2	Secure Shell (SSH) Protocol permission flag. (0=SSH is not supported, 1= SSH is supported). "Supporting SSH" means the Avaya Services organization can have remote access to the deskphone, using SSHv2, as described in topic Secure Shell Support. When value =2, SSH will still be disabled by default (i.e., the SSH server listen port will be closed), but SSH will be able to be manually enabled (or disabled if it was previously manually enabled) from the Craft Debug procedure.
SSH_BANNER_FILE	Null	Specifies the file name or URL for a custom SSH banner file. Zero to 255 ASCII characters: zero or one file name or URL. Used to provide a security warning message to the client before SSH authentication is attempted. If the parameters is left at the default value, the default banner message is as stated in the topic Secure Shell Support.
SSH_IDLE_TIMEOUT	10	Specifies the number of minutes of inactivity after which SSH will be disabled. Valid values are 1 to 5 ASCII numeric digits, zero through 32767.
SSH_LOCKOUT_ATTEMPTS	0	Specifies the number of failed login attempts after which SSH will be disabled. Valid values are 1 to 5 ASCII numeric digits, zero through 32767.
SSH_LOGIN_DELAY	60	Specifies the number of seconds of delay between login attempts if three or more attempts fail. Valid values are 1 to 5 ASCII numeric digits, zero through 32767.
SSH_USERNAME	"craft"	Specifies the user name to be used for SSH logins. Valid values are 0 to 255 ASCII characters.
SSO_ENABLED	0	Specifies whether Single Sign (SSO) on capability is enabled or disabled. Valid values are: <ul style="list-style-type: none">• 0: Default, SSO disabled.• 1: SSO enabled.

Table continues...


Parameter name	Default value	Description and value range
SSO_CLIENT_CERT	0	<p>Specifies whether the telephone will request and authenticate an identity certificate from the desktop computer during the TLS handshake for SSO. Valid values are:</p> <ul style="list-style-type: none"> • 0: Default value, specifies that the telephone will not request a certificate from the desktop computer. • 1: The telephone will request and authenticate an identity certificate from the desktop computer during the TLS handshake.
SSO_DISCONNECT_ACTION	1	<p>Specifies what the telephone does if the link is lost on the secondary (PC) Ethernet interface while it is registered with credentials that were provided by, or that are the same as those provided by, an SSO Register command. Valid values are:</p> <ul style="list-style-type: none"> • 1: Default, the telephone invokes each FAC contained in the value of SSO_DISCONNECT_FACS and then unregisters. • 2: The telephone locks up. • 3: The telephone remains active. <p> Note:</p> <p>If the SSO TCP connection is terminated but the link is not lost, no action is taken based on this parameter.</p>
SSO_DISCONNECT_FACS	Null	Specifies a list of Feature Access Codes (FACs) to be activated before the deskphone unregisters due to loss of the SSO-LD link.
SSO_LOCK_SYNC	1	<p>Specifies what the telephone does if the telephone receives a Lock or Unlock command from the SSO application. Valid values are:</p> <ul style="list-style-type: none"> • 0: The telephone ignores the LOCK command. • 1: Default, the telephone attempts to run the LOCK command.

Table continues...

Parameter name	Default value	Description and value range
SSO_REGISTERED_MODE	1	<p>Specifies what the telephone does if the telephone receives a Register command from an SSO application when the telephone is already registered. Valid values are 1, 2.</p> <ul style="list-style-type: none"> • 1: Default, the telephone unregisters and attempts a normal registration using the received credentials. If the new credentials match the existing credentials, the telephone will not unregister and reregister. • 2: The telephone accepts the received credentials only if the credentials match the existing credentials.
SIG	0	<p>Signaling protocol download flag. Valid values are:</p> <p>0 = Default. Default means to download the upgrade file for the same protocol that is supported by the software that the deskphone is currently using.</p> <ul style="list-style-type: none"> • 1: Use H.323 protocol. • 2: Use SIP protocol.
SNMPADD	Null	Text string containing zero or more allowable source IP addresses for SNMP queries, in dotted decimal or DNS format, separated by commas, with up to 255 total ASCII characters including commas.
SNMPSTRING	Null	Text string containing the SNMP community name string (up to 32 ASCII characters, no spaces). The SNMP community string can also be administered on the system-parameters IP-options form.

Table continues...


Parameter name	Default value	Description and value range
SYSAUDIOPATH	0	<p>For Avaya Call Center use only</p> <p>Specifies whether the agent can select an option for Audio Path (the Headset or Speaker) or must use the default as configured by the administrator. Valid values are:</p> <ul style="list-style-type: none"> • 0: Default value. The agent can select the audio path by going to Options & Settings > Call Settings. The options are Headset or speaker. • 1: The deskphone automatically sets the parameter OPTAUDIOPATH to 1 (speaker) and the agent will not have the option to choose the audio path through call settings. • 2: The deskphone automatically sets parameter OPTAUDIOPATH to 2 (headset) and the agent will not have the option to choose the audio path through call settings. <p> Note:</p> <p>By implication, if the <code>46xxsettings.txt</code> file contains a non-default value for SYSAUDIOPATH, the setting for SYSAUDIOPATH overrides any user-specified settings for the audio path.</p>
TIMERSTAT	0	<p>TIMERSTAT specifies whether Timer On and Timer Off softkeys will be presented to the user.</p> <ul style="list-style-type: none"> • 0: Timer On and Timer Off softkeys will not be presented to the user (default). • 1: Timer On and Timer Off softkeys will be presented to the user.
TLSDIR	Null	<p>HTTPS server directory path. The path name prepended to all file names used in HTTPS get operations during initialization. Value: 0-127 ASCII characters, no spaces. Null is a valid value. Leading or trailing slashes are not required. The command syntax is <i>SET TLSDIR mytlsdir</i> where <i>mytlsdir</i> is your HTTPS server path. TLSDIR is the path for all HTTPS operations except for BRURI.</p>
TLSPORT	411	<p>TCP port number used for HTTPS file downloading. 2 to 5 ASCII numeric digits. Valid values are 80 through 65535. Note that when the file server is on Communication Manager, set this value to 411 which is the port required for HTTPS downloads rather than the using the default.</p>

Table continues...

Parameter name	Default value	Description and value range
TLS_SECURE_RENEG	0	Specifies whether a TLS session should be terminated if the peer does not support secure renegotiation. Valid values are: <ul style="list-style-type: none"> • 0: TLS secure renegotiation is not required from peer. • 1: TLS secure renegotiation is required from peer.
TLSSRVR	Null	IP addresses or DNS Names of HTTPS file servers used to download deskphone files. Dotted decimal or DNS format, separated by commas. Valid values are 0-255 ASCII characters, including commas.
TLSSRVRVERIFYID	0	Specifies whether the identity of a TLS server is checked against its certificate. The identity of the server is checked with the common name or subjectAltName fields in the server certificate. Valid values are: <ul style="list-style-type: none"> • 0: Identity of a TLS server is not checked against its certificate. • 1: Identity of a TLS server is checked against its certificate. The validation of server identity is applicable for IPSec VPN with certificate based authentication (using NVSGIP), Backup/restore over HTTPS (using BRURI), HTTPS file server (using TLSSRVR), WML browser (using WMLHOME), H.323 over TLS signaling (using MCIPADD).
TLS_VERSION	0	Controls the TLS version that is used for all TLS connections. Valid values are: <ul style="list-style-type: none"> • 0: TLS versions 1.0, 1.1, and 1.2 are supported with TLS v1.2 as default. • 1: TLS 1.0 and TLS 1.1 are not supported. Only TLS v1.2 and higher are permitted.
UDT	10	Specifies the Unsuccessful Discovery Timer (UDT) in minutes. UDT is the time that the phone perform discovery with list of gatekeepers configured and after which the phone will reboot if no gatekeeper from the list is discovered. Valid values are 10 to 960.
VPNALLOWTAGS	0	Specifies whether 802.1Q tags (controlled by L2Q parameter) can be used in VPN mode. Valid values are:
VUMCIPADD	Null	Specifies a list of H.323 call server IP addresses for the Visiting User feature. addresses can be in dotted-decimal (IPv4) or DNS name format, separated by commas without any intervening spaces. The list can contain up to 255 characters

Table continues...

Parameter name	Default value	Description and value range
WBCSTAT	1	Valid values are 1 to 6. <ul style="list-style-type: none"> • 0: Tags not allowed in the VPN mode. • 1: Tags allowed in the VPN mode. Specifies whether a wideband codec indication will be displayed when a wideband codec is being used.
XFERSTAT	0	Specifies whether the Transfer button is enabled or disabled when CCBTNSTAT is 0. Valid values are: <ul style="list-style-type: none"> • 0: The Transfer button is disabled when CCBTNSTAT is 0. • 1: The Transfer button is enabled.

*** Note:**

The preceding table applies to all IP deskphones. Certain IP deskphones might have additional optional information that you can administer.

Single Sign on for local devices (SSON-LD)

With the Single Sign On for local devices (SSON-LD) feature, you can log in to your desktop computer and then automatically log in to your deskphone using separate phone login credentials.

When you log out of the desktop computer, the connected deskphone also locks up.

To use this feature:

- Your administrator must enable the SSO-LD feature for your extension.
- Your desktop computer must have an SSO-LD application installed.
- You must connect your desktop computer to your deskphone through the secondary LAN interface on the deskphone.

You can use the SSO-LD feature in the following scenarios:

- Office: When you log in to a computer that you have connected to your office deskphone, or when you reconnect your laptop to your office deskphone, the deskphone automatically unlocks, and logs you in. When you turn off the computer and disconnect the computer the deskphone automatically locks up. The deskphone does not log out and continues to log missed calls.
- Shared public desk: When a user, for example, a guest, connects the office laptop to a deskphone at a public desk, the deskphone automatically registers and the phone is unlocked. When a user disconnects the laptop, the deskphone automatically unregisters or locks. If the user reconnects to the same deskphone, the deskphone automatically reregisters or unlocks.
- Conference room: This scenario is similar to that at a public desk, but when the user disconnects the laptop, the deskphone reregisters with the room extension.

- Shared desk with shared computer: This scenario is similar to a desktop computer connected to an office phone. However in this case, the desktop computer supports multiple user login accounts as users share the PC and the phone by working on different shifts.
- Contact center: The desktop computer connected to the deskphone runs a contact center program. When an agent logs in to the computer, the phone automatically registers the user to a call server. The agent must log in to the call center separately. The agent also has the option to log in through an agent login Feature Access Code (FAC) to the contact center program. When the agent logs out of the computer, the phone unregisters, and hence, the agent logs out of the call center.

Administering a VLAN

This section contains information on how to administer Avaya J100 Series IP Phones to minimize registration time and maximize performance in a Virtual LAN (VLAN) environment. If your LAN environment does not include VLANs, set the system parameter L2Q to 2 (off) to ensure correct operation.

Related links

[About VLAN Tagging](#) on page 166

[The VLAN default value and priority tagging](#) on page 166

[Automatic detection of a VLAN](#) on page 167

About VLAN Tagging

IEEE 802.1Q tagging (VLAN) is a useful method of managing VoIP traffic in your LAN. You can establish a *voice* VLAN, set L2QVLAN to the VLAN ID of that VLAN, and provide voice traffic with priority over other traffic. If LLDP was used to set the VLAN for the deskphones, that setting has absolute authority. Otherwise, you can set VLAN tagging manually, by DHCP, or in the 46xxsettings.txt file.

If VLAN tagging is enabled (L2Q=0 or 1), the IP Deskphones set the VLAN ID to L2QVLAN, and VLAN priority for packets from the deskphone to L2QAUD for audio packets and L2QSIG for signaling packets. The default value (6) for these parameters is the recommended value for voice traffic in IEEE 802.1D.

Regardless of the tagging setting, a IP Deskphone will always transmit packets from the deskphone at absolute priority over packets from the secondary Ethernet interface from an attached PC. The priority settings are useful only if the downstream equipment is administered to give the *voice* VLAN priority.

Related links

[Administering a VLAN](#) on page 166

The VLAN default value and priority tagging

The parameter L2QVLAN identifies the 802.1Q VLAN Identifier and is initially set to 0. This default value indicates *priority tagging* and specifies that your network Ethernet switch automatically insert the default VLAN ID without changing the user priority of the frame.

But some switches do not process a VLAN ID of zero and require frames tagged with a non-zero VLAN ID.

If you do not want the default VLAN to be used for voice traffic, set the value of L2QVLAN to the VLAN ID appropriate for your voice LAN.

You can also administer another parameter VLANTEST that defines the number of seconds the phone waits for a DHCPOFFER message when using a non-zero VLAN ID. The VLANTEST default is 60 seconds. If you use VLANTEST, the deskphone returns to the default VLAN if an invalid VLAN ID is administered or if the phone moves to a port where the L2QVLAN value is invalid.

The default value of VLANTEST is long, allowing for the scenario that a major power interruption is causing the phones to restart. Always allow time for network routers, the DHCP servers, and other equipment to be returned to service. If the deskphone restarts for any reason and the VLANTEST time limit expires, the administered VLAN ID becomes invalid. The deskphone then initiates operation with a VLAN ID of 0. Or, if the value of L2Q is 0, that is auto, the deskphone turns off tagging until the L2QVLAN is set to a non-zero value or until the deskphone verifies that the network can support tagged frames.

Setting VLANTEST to "0" causes the phone to use a non-zero VLAN indefinitely to attempt DHCP. In other words, the deskphone does not return to the default VLAN.

Related links

[Administering a VLAN](#) on page 166

Automatic detection of a VLAN

The phones support automatic detection of the L2QVLAN setting that is incorrect. When the value of L2QVLAN is not 0 and VLAN tagging is enabled, L2Q= 0 or 1, initially the IP Deskphone transmits DHCP messages with IEEE 802.1Q tagging and sets the VLAN ID to L2QVLAN. The phones will continue to do this for number of seconds configured by VLANTEST.

- If L2Q=1 and the VLANTEST timer expires because the phone has not received a DHCPOFFER, the phone sets L2QVLAN=0 and transmits DHCP messages with the default VLAN (0).
- If L2Q=0 and the VLANTEST timer expires because the phone has not received a DHCPOFFER, the phone sets L2QVLAN=0 and transmits DHCP messages without tagging.
- If VLANTEST is 0, the timer never expires.

Note:

Regardless of the setting of L2Q, VLANTEST, or L2QVLAN, you must have administer DHCP on the phone so that the phone receives a response to a DHCPDISCOVER on making that request on the default (0) VLAN.

After VLANTEST expires, if the phone receives a non-zero L2QVLAN value, the phone releases the IP address and sends DHCPDISCOVER on that VLAN. Any other release requires you to perform a manual reset before the phone attempts to use a VLAN on which VLANTEST has expired.

The phone ignores any VLAN ID administered on the call server if a non-zero VLAN ID is administered either by LLDP, manually, through DHCP, or through the settings file.

Related links

[Administering a VLAN](#) on page 166

About DNS addressing

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

Note:

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

EAP-TLS support for authentication

You can use the EAP-TLS as the mode of authentication. To activate this mode, you must add a new parameter DOT1XEAPS, with valid values of MD5 or TLS to the settings file. The default value is MD5. The call server supports EAP-TLS as specified in RFC 2716 if and only if an identity certificate is present in the deskphone and if the value of DOT1XEAPS is TLS. If an EAP method requires the authentication of a digital certificate, and if you have enabled the Supplicant on the phone and the value of DOT1XEAPS changes, the Supplicant will transmit an EAPOL-Logoff message and return to the CONNECTING state.

Related links

[Enabling certificate support](#) on page 168

[Activating EAP-TLS for authentication](#) on page 169

[Scenarios for using EAP-TLS based authentication](#) on page 170

[Deploying EAP-TLS based authentication for phones using 802.1x and MD5](#) on page 170

[Deploying EAP-TLS on phones running without any type of 802.1x authentication](#) on page 172

Enabling certificate support

You can use Simple Certificate Enrollment Protocol (SCEP) to provide an identity certificate for use with certificate-based VPN authentication methods. The 802.1x EAP-TLS method also uses the identity certificate for authentication. When you use TLS with HTTPS, you can use the identity certificate to authenticate the phone and save the agent greetings or perform a backup or restore.

The phone stores the identity certificate and the phone uses the identity certificate during the TLS handshake as required when the phone is acting as a server. When the phone is acting as a client, the phone transmits the identity certificate on request. The IP Deskphones support Media Encryption (SRTP) and use built-in Avaya certificates for trust management. Trust management includes downloading certificates and managing policies for additional trusted Certificate Authorities (CA). Simple Certificate Enrollment Protocol (SCEP) handles identity management with phone certificates and private keys. You can apply SCEP to your VPN operation or to standard enterprise network operation. Alternatively, you can download the PKCS #12 file that contains an identity certificate and its private key. You must enter the authentication password after reboot.

Before you begin

For SCEP servers that are outside the corporate firewall, configure the phones that use a VPN connection to establish an SCEP connection through an HTTP proxy server to reach the SCEP server. In this instance, use the WMLPROXY system parameter to configure the HTTP proxy server.

When the phone initiates SCEP, the phone attempts to contact an SCEP server through HTTP, using the value of the configuration parameter MYCERTURL as the URI. SCEP supports an HTTP proxy server. The phone creates a private/public key pair, where the length of each key is equal to the value of the configuration parameter MYCERTKEYLEN. The certificate request uses the public key and the values of the configuration parameters MYCERTCAID, MYCERTCN, MYCERTDN, and SCEPPASSWORD.

About this task

You must configure the `46xxsettings.txt` file on the file server with the specified parameters to use an identity certificate to authenticate the phones.

Procedure

Configure the following parameters in the `46xxsettings.txt` file:

- SET MYCERTURL < URL for enrolling with a SCEP fronted Certificate Authority> for example, `http://149.49.44.53/certsrv/mscep/mscep.dll`.
- SET MYCERTCN \$MACADDR.
- SET MYCERTWAIT 1.
- SET TRUSTCERTS "root_certificate".

Related links

[EAP-TLS support for authentication](#) on page 168

Activating EAP-TLS for authentication

Before you begin

To activate the 802.1x EAP-TLS mode, you must "SET DOT1XEAPS TLS on the `46xxsettings.txt` file of the file server.

About this task

You can use the EAP-TLS method to authenticate the phones with the call server. For implementing this type of authentication, you must configure the EAP-TLS parameters in the `46xxsettings.txt` file and on the call server.

Procedure

1. SET MYCERTURL < URL for enrolling with a SCEP fronted Certificate Authority >. URL Example: `http://149.49.44.53/certsrv/mscep/mscep.dll`.
2. SET MYCERTWAIT 1
3. SET MYCERTCN \$MACADDR
4. SET DOT1XEAPS TLS
5. SET TRUSTCERTS & <Root CA Filename>
6. Connect the phone to a port that does not have 802.1x enabled. The phone receives the settings from the `46xxsettings.txt` file.
The phone contacts the call server to activate the SCEP process.
7. Unplug the phone and connect the phone to a port that you have configured for EAP-TLS and enable the supplicant on the phone through the CRAFT procedure. You can also enable the supplicant by configuring the `46xxsettings.txt` with `SET DOT1XSTAT 2`.

Note:

The MAC option `SET MYCERTCN $MACADDR` supports the MYCERTCN parameter in H.323 Release 6.2 Service Pack 1.

For H.323 Release 6.2 Service Pack 1, after the phone starts with EAP-TLS mode, the user does not need to enter device Id or password as in MD5.

Related links

[EAP-TLS support for authentication](#) on page 168

Scenarios for using EAP-TLS based authentication

You can deploy the EAP-TLS method for authentication that requires an identity certificate that is stored in the phone.

The following sections describe the authentication scenarios where you might need to deploy EAP-TLS. Before deploying EAP-TLS, you must set the phones to a default state that can be one of the following:.

- Phones not running any type of 802.1x authentication
- Phones using 802.1x using MD5 as the authentication method

Related links

[EAP-TLS support for authentication](#) on page 168

Deploying EAP-TLS based authentication for phones using 802.1x and MD5

Before you begin

The administration of EAP-TLS requires the installation of an identity certificate. So, the initial network for phone installation can be a phone, an Ethernet switch, and a computer in the IT department. The computer must be connected to the internet if you use an external CA for signing

the certificates. You can configure the settings file on the network to configure DOT1XSTAT to 1 or 2. This change takes effect the next time that the phone resets. The phone must be connected to that network without resetting until a certificate is successfully installed. Or, you can enable 802.1x manually by using the 802.1x craft procedure after you install a certificate.

Procedure

1. Clear the phones and ensure that the phones authenticate using MD5.
2. Connect the phones on a network that does not support 802.1X access control (switch and phone), modify the `46xxsettings.txt` file, and incorporate the following SCEP parameters:
 - a. SET TRUSTCERTS < RootCert >
 - b. SET MYCERTURL http:// <IP of CA server > /certsrv/mscep/mscep.dll
 - c. SET MYCERTWAIT 0
 - d. SET SCEPPASSWORD <password>##### optional
 - e. SET DOT1XEAPS TLS
 - f. SET DOT1XSTAT 2 ##### optional
- g. Clear the phone and then restart the phone, and ensure that the phone upgrades to the latest firmware available.
- h. Connect the phone to a network that supports DOT1x.

The phone starts the process of certificate enrollment automatically, by sending a SCEP request to MYCERTURL. After the boot process completes, the phone obtains the root certificate and the device certificate successfully and changes to the EAP-TLS mode.

Note:

When you install the identity certificate using SCEP, you can download the PKCS12 file.

- i. Monitor the CA, to check that all phones that you have upgraded, have enrolled their certificates with the CA. If you administer the CA to require manual approval of certificate enrollment requests, then the phone will take a minimum of two minutes to download the enrolled certificate after the CA approves the request. Therefore, do not restart the phones until at least 2 minutes after approving the certificate enrollment request. If the certificate enrollment process is automatic, it takes less time than manual enrollment.
3. Administer the RADIUS server to accept the identity certificates provided by the phones.
4. To turn on 802.1x authentication, change the `46xxsettings.txt` file by setting DOT1XSTAT to a value of 1 or 2.
5. Restart the phones to apply the new settings. The phones start their supplicants with the EAP-TLS authentication method. Configure the Layer 2 switches to which you attach these phones. The switches can then support EAP-TLS on those ports to which you attach the phones.

If you do not require the phone to connect to a network that does not support DOT1X , reset the phones manually or using the CM and only then, change the switch configuration to support EAP-TLS.

Result

The switches then prompt the phones to authenticate using EAP-TLS and the phones must authenticate themselves using the enrolled certificates. After you setup the phones, the phones must maintain their configurations across restarts and upgrades. Depending on the value of MYCERTRENEW, the phones try to renew their certificates enrollment, periodically. The administrator must monitor pending enrollments.

Related links

[EAP-TLS support for authentication](#) on page 168

Deploying EAP-TLS on phones running without any type of 802.1x authentication

Before you begin

Configure the Layer 2 switches to which you attach the phones running without any type of 802.1x authentication, so that the switches do not support EAP-TLS on the ports to which the phones are attached.

Procedure

1. Clear the phones and then in the `46xxsettings.txt` file, turn off the supplicant operation by making the following entry: `SET DOT1XSTAT 0`.
2. Modify the `upgrade.txt` file to point to location for the H.323 Release 6.2 Service Pack 1 files.
3. Modify the settings file, to incorporate the following SCEP parameters appropriately: MYCERTURL, MYCERTWAIT, MYCERTRENEW and MYCERTDN if needed.
4. Reboot the phone, and ensure that the phone upgrades to H.323 Release 6.2 Service Pack 1. The phone starts the process of certificate enrollment automatically, by sending a SCEP request to MYCERTURL.
5. Monitor the CA, to check whether all the phones that the system has upgraded, have enrolled their certificates with the CA.

Note:

If you administer the CA to require manual approval of certificate requests, then the phone takes a minimum of two minutes to download the identity certificate after the CA approves the request. Therefore, do not reboot the phones until at least two minutes after approving the certificate enrollment request. If the certificate enrollment process is automatic, the process takes less time than manual enrollment.

6. Administer the RADIUS server to accept the identity certificates provided by the phones.
7. Change the `46xxsettings.txt` file, to turn on 802.1x authentication, by setting DOT1XSTAT to a value of 1 or 2.

8. Set the EAPS authentication method to TLS by setting `SET DOT1XEAPS TLS` in the `46xxsettings.txt` file.
9. Configure the Layer 2 switches to which you have attached these phones, to support EAP-TLS on the ports to which you have attached the phones.

Result

The switches prompt the phones to authenticate using EAP-TLS and the phones authenticate using the enrolled certificates. After setup completes, the phones maintain the configurations across restarts and upgrades. Depending on the value of `MYCERTRENEW`, the phones try to renew their certificates enrollment, periodically. The administrator must monitor pending enrollments.

Related links

[EAP-TLS support for authentication](#) on page 168

About IEEE 802.1X

IP phones support the IEEE 802.1X standard for Supplicant operation and support pass-through of 802.1X messages to an attached PC. The system parameter `DOT1X` determines how the phones handle pass-through of 802.1X multicast packets and proxy logoff:

- When `DOT1X = 0`, the phone forwards 802.1X multicast packets from the Authenticator to the PC attached to the phone and forwards multicast packets from the attached PC to the Authenticator (multicast pass-through). The phone does not support Proxy Logoff. This is the default value.
- When `DOT1X = 1`, the phone supports the same multicast pass-through as when `DOT1X=0`, but Proxy Logoff is also supported. When the secondary Ethernet interface loses link integrity, the phone sends an 802.1X EAPOL-Logoff message to the Authenticator with a source MAC address from the previously attached device. This message alerts the Authenticator that the device is no longer connected.
- When `DOT1X = 2`, the phone forwards multicast packets from the Authenticator only to the phone, ignoring multicast packets from the attached PC (no multicast pass-through). The phone does not support Proxy Logoff.
- Regardless of the `DOT1X` setting, the phone always properly directs unicast packets from the Authenticator to the phone or its attached PC as specified by the destination MAC address in the packet.

All IP phones support Supplicant operation as specified in IEEE 802.1X, but, as of software Release 2.0, only if the value of the parameter `DOT1XSTAT` is 1 or 2. If `DOT1XSTAT` has any other value, the phone does not support Supplicant operation.

Unicast 802.1X frames contain the MAC address of the phone as the destination MAC address and a protocol type of 88-8E hex. IP phones respond to unicast 802.1X frames received on the Ethernet line interface if the value of `DOT1XSTAT` is 1 or 2.

IP phones respond to 802.1X frames that have the PAE group multicast address as the destination MAC address only if the value of `DOT1XSTAT` is 2. If the value of `DOT1XSTAT` is

changed to 0 from any other value after the Supplicant has been authenticated, an EAPOL-Logoff will be transmitted before the Supplicant is disabled.

From Release 2.0 onwards, the system parameter DOT1XSTAT determines how the phone handles Supplicants as follows:

- When DOT1XSTAT = 0, Supplicant operation is completely disabled. This is the default value.
- When DOT1XSTAT = 1, Supplicant operation is enabled, but responds only to received unicast EAPOL messages.
- When DOT1XSTAT = 2, Supplicant operation is enabled and responds to received unicast and multicast EAPOL messages.

 **Note:**

If the Ethernet line interface link fails, the 802.1X Supplicant, if enabled, enters the Disconnected state.

Related links

[802.1X supplicant operation](#) on page 174

802.1X supplicant operation

IP phone that support supplicant operation also support Extensible Authentication Protocol (EAP). For software Release 6.1 and earlier, only the MD5-Challenge authentication method is supported. For more information about the MD5-Challenge authentication, see IETF RFC 3748.

A supplicant identity (ID) and password of not more than 12 numeric characters are stored in reprogrammable non-volatile memory. The phone software downloads do not overwrite the ID and password. The default ID is the MAC address of the phone, converted to ASCII format without colon separators, and the default password is null. Both the ID and password are set to default values at manufacture. EAP-Response/Identity frames use the ID in the Type-Data field. EAP-Response/MD5-Challenge frames use the password to compute the digest for the Value field, leaving the Name field blank.

When you install a phone for the first time and 802.1x is in effect, the dynamic address process prompts the installer to enter the supplicant identity and password. The IP phone does not accept null value passwords.

The IP deskphone stores 802.1X credentials when the phone achieves successful authentication. Post-installation authentication attempts occur using the stored 802.1X credentials, without prompting the user for ID and password entry.

An IP deskphone can support several different 802.1X authentication scenarios, depending on the capabilities of the Ethernet data switch to which the deskphone is connected. Some switches might authenticate only a single device per switch port. This operation is known as single-supplicant or port-based operation. These switches usually send multicast 802.1X packets to authenticating devices.

These switches support the following three scenarios:

- Standalone phone (Deskphone Only Authenticates) - When you configure the IP phone for supplicant mode (DOT1XSTAT=2), the phone can support authentication from the switch.
- Phone with attached PC (Deskphone Only Authenticates) - When you configure the IP phone for supplicant mode (DOT1X=2 and DOT1XSTAT=2), the phone can support authentication from the switch. The attached computer in this scenario gains access to the network without being authenticated.
- Deskphone with attached computer (PC Only Authenticates) - When the IPdeskphone is configured for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1 and DOT1XSTAT=0), an attached PC running 802.1X supplicant software can be authenticated by the data switch. The phone in this scenario gains access to the network without authentication.

Some switches support authentication of multiple devices connected through a single switch port. This operation is known as multi-supplicant or MAC-based operation. These switches usually send unicast 802.1X packets to authenticating devices. These switches support the following two scenarios:

- Standalone phone (Deskphone Only Authenticates) - When you configure the IP phone for supplicant mode (DOT1XSTAT=2), the phone can support authentication from the switch. When DOT1X is "0" or "1" the phone cannot authenticate with the switch.
- Phone and computer Dual Authentication - Both the IP phone and the connected computer can support 802.1X authentication from the switch. You can configure the IP phone for Pass-Through Mode or Pass-Through Mode with Logoff (DOT1X=0 or 1 and DOT1XSTAT=1 or 2). The attached computer must be running 802.1X supplicant software.

Related links

[About IEEE 802.1X](#) on page 173

About Link Layer Discovery Protocol (LLDP)

Link Layer Discovery Protocol (LLDP) is an open standards layer 2 protocol that IP phones use to advertise their identity and capabilities and to receive administration from an LLDP server. LAN equipment can use LLDP to manage power, administer VLANs, and provide some administration.

IEEE 802.1AB-2005 specifies the transmission and reception of LLDP. The phone use Type-Length-Value (TLV) elements specified in IEEE 802.1AB-2005, TIA TR-41 Committee - Media Endpoint Discovery (LLDP-MED, ANSI/TIA-1057), and Proprietary elements. LLDP Data Units (LLDPDUs) are sent to the LLDP Multicast MAC address (01:80:c2:00:00:0e).

These phones:

- do not support LLDP on the secondary Ethernet interface.
- do not forward frames received with the 802.1AB LLDP group multicast address as the destination MAC address between the Ethernet line interface and the secondary Ethernet interface.

The phone initiates LLDP after receiving an LLDPDU message from an appropriate system. After the phone is initiated, the phone sends an LLDPDU every 30 seconds or as specified by LLDP_XMIT_SECS parameter with the following contents:

Table 12: LLDPDU transmitted by the phones

Category	TLV Name (Type)	TLV Info String (Value)
Basic Mandatory	Chassis ID	IPv4 IP Address of phone.
Basic Mandatory	Port ID	MAC address of the phone.
Basic Mandatory	Time-To-Live	120 seconds.
Basic Optional	System Name	The Host Name sent to the DHCP server in DHCP option 12.
Basic Optional	System Capabilities	Bit 2 (Bridge) is set in the System Capabilities if the phone has an internal Ethernet switch. If Bit 2 is set in Enabled Capabilities then the secondary port is enabled. Bit 5 (phone) in the System Capabilities. If Bit 5 is set in the Enabled Capabilities then the phone is registered.
Basic Optional	Management Address	Mgmt IPv4 IP Address of phone. Interface number subtype = 3 (system port). Interface number = 1. OID = SNMP MIB-II sysObjectID of the phone.
IEEE 802.3 Organization Specific	MAC / PHY Configuration / Status	Reports auto-negotiation status and speed of the uplink port on the phone.
TIA LLDP MED	LLDP-MED Capabilities	Media Endpoint Discovery - Class III - IP Telephone.
TIA LLDP MED	Extended Power-Via-MDI	Power Value = 0 if the phone is not currently powered through PoE, else the maximum power usage of the deskphone plus all modules and adjuncts powered by the phone in tenths of a watt.
TIA LLDP MED	Network Policy	Tagging Yes/No, VLAN ID for voice, L2 Priority, DSCP Value.
TIA LLDP MED	Inventory – Hardware Revision	MODEL - Full Model Name.
TIA LLDP MED	Inventory – Serial Number	Phone serial number.
TIA LLDP MED	Inventory – Manufacturer Name	Avaya.
TIA LLDP MED	Inventory – Model Name	MODEL with the final D xxx characters removed.
Avaya Proprietary	PoE Conservation Level Support	Provides power conservation abilities and settings, Typical and Maximum Power values. OUI = 00-40-0D (hex), Subtype = 1.

Table continues...

Category	TLV Name (Type)	TLV Info String (Value)
Avaya Proprietary	Call Server IP Address	Call Server IP address. Subtype = 3.
Avaya Proprietary	IP Phone Addresses	Phone IP address, Phone address mask, Gateway IP address. Subtype = 4.
Avaya Proprietary	File Server	File Server IP address. Subtype = 6.
Avaya Proprietary	802.1Q Framing	802.1Q Framing = 1 if tagging or 2 if not. Subtype = 7.
Basic Mandatory	End-of-LLDPDU	Not applicable.

On receipt of a LLDPDU message, the phones will act on the TLV elements described in the following table:

Table 13: Impact of TLVs Received by System Parameter Values

System Parameter Name	TLV Name	Impact
PHY2VLAN	IEEE 802.1 Port VLAN ID	The value is changed to the Port VLAN identifier in the TLV.

Table continues...

System Parameter Name	TLV Name	Impact
L2QVLAN and L2Q	IEEE 802.1 VLAN Name	<p>The value is changed to the TLV VLAN Identifier. L2Q will be set to 1 (ON). VLAN Name TLV is only effective if the following conditions are met:</p> <ul style="list-style-type: none"> • The phone is not registered with the call server. • Name begins with VOICE (letters are not case-sensitive). • The VLAN is not zero. • DHCP Client is activated. • The phone is registered but is not tagging layer 2 frames with a non-zero VLAN ID. <p>If VLAN Name causes the phone to change VLAN and the phone already has an IP Address the phone will release the IP Address and reset.</p> <p>If the TLV VLAN ID matches the VLAN ID the phone is using, the VLAN ID is marked as set by LLDP. Otherwise, if already registered, the phone waits until there are no active calls, releases its IP Address, turns on tagging with the TLV VLAN ID, sets L2Q to <i>on</i> changes the default L2Q to <i>on</i> and resets. If there is no valid IP Address, the phone immediately starts tagging with the new VLAN ID without resetting.</p>
L2Q, L2QVLAN, L2QAUD, L2QSIG, DSCPAUD, DSCPSIG	MED Network Policy TLV	<p>L2Q - set to 2 (off) If T (the Tagged Flag) is set to 0; set to 1 (on) if T is set to 1.</p> <p>L2QVLAN - set to the VLAN ID in the TLV.</p> <p>L2QAUD and L2QSIG - set to the Layer 2 Priority value in the TLV.</p> <p>DSCPAUD and DSCPSIG - set to the DSCP value in the TLV.</p> <p>The system checks whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. This TLV is ignored if:</p> <ul style="list-style-type: none"> • the value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0, or • the Application Type is not 1 (Voice), or • the Unknown Policy Flag (U) is set to 1.
MCIPADD	Proprietary Call Server TLV	MCIPADD will be set to this value if it has not already been set.
TLSSRVR and HTTPSRVR	Proprietary File Server TLV	TLSSRVR and HTTPSRVR will be set to this value if neither of them have already been set.

Table continues...

System Parameter Name	TLV Name	Impact
L2Q	Proprietary 802.1 Q Framing	<p>The default L2Q is set to the value of this TLV. No change is made to the current L2 tagging, but the new default value is used on the next reboot.</p> <ul style="list-style-type: none"> • If the 802.1Q Framing value is 1, L2Q will be set to “1” (on) • If the 802.1Q Framing value is 2, L2Q will be set to “2” (off) • If the 802.1Q Framing value is 3, L2Q will be set to “0” (auto)
	Proprietary - PoE Conservation TLV	This proprietary TLV can initiate a power conservation mode. The phones that support this will turn the phone backlight and the backlight of an attached Button Module on or off in response to this TLV.
	Extended Power-Via-MDI	Power conservation mode is enabled if the received binary Power Source value is 10, and power conservation mode is disabled if the received binary Power Source value is not 10. Power conservation mode is enabled even if the phone is not powered over Ethernet because the phone sends information about the power source that it is using in a TIA LLDP MED Extended Power-Via-MDI TLV. The power management system intends to conserve local power also.

Administering settings at the phone

The guide describes how to use Craft local procedures at the phone for administration. The local procedures you might use as an administrator are:

- 802.1x - Enable or disable the Supplicant and the Pass-thru options.
- AGC - Enable/disable Automatic Gain Control.
- ADDR - Add the IP addresses for the call server, HTTP server, HTTPS server, and other network related parameters.
- CLEAR - Remove all administered values, user-specified data, option settings, etc. and return a phone to the phone's initial “out of the box” default values.
- CONT - Adjust the contrast of button modules.
- DEBUG - Enable or disable debug mode for the button module serial port and other debug options.
- GROUP - Set the group identifier on a per-phone basis.
- LOG - Enable/disable event logging.
- LOGOUT - Log off the deskphone.

- MLS - View multi-language text strings.
- SIG - Set the signaling protocol.
- HSEQUAL - Administer the HAC related parameters.
- INT - Set or change the interface control value(s) of PHY1STAT and/or PHY2STAT.
- RESET VALUES- Reset the deskphone to default values including any values administered through local procedures, and the values previously downloaded using DHCP or a settings file.
- RESTART PHONE- Restart the deskphone in response to an error condition, including the option to reset parameter values.
- SSON - To add site specific options.
- Test - To run a self test on the phone.
- VIEW - Review system parameters to verify the current parameter values and file versions.
- VPN - Administer VPN settings.



Note:

If you have not changed the default password, the Debug option is available in a Read-Only mode.

You can use the DEBUG option only if you change the default password to the Craft local procedures through the PROCPSWD parameter.

The new value of the PROCPSWD parameter must be 4 to 7 numeric digits, "0000" through "9999999". However, if value of PROCPSWD is less than 4 digits after you install Release 6.2.4 or later, the value will be changed back to the default value of 27238.

Administering display language options

By default, the phone displays information in the English language.

All software downloads include language files for 19 languages.

Administrators can specify from one to four languages for each phone to replace English. Users can then select the language in which the phone displays messages.

All downloadable language files contain all information needed for the phone to present the language as part of the user interface.

Use the configuration file and the following parameters to customize the settings for up to four languages:

- LANGxFILE - The name of a selected language file, for example, *French*. In addition to providing the language name as this value, replace the x in this parameter with a 1, 2, 3, or 4 to indicate which of the four languages you are specifying. For example, to indicate that German and French are the available languages, the setting is:
`LANG1FILE=mlf_german.txt` and `LANG2FILE=mlf_french.txt`.

- LANG0STAT - Use this parameter to select the built-in English language when other languages are downloaded. If LANG0STAT is 0 and at least one language is downloaded, you cannot select the built-in English language. If LANG0STAT is 1 then you can select the built-in English language text strings.
- LANGSYS - The file name of the system default language file, if any.
- LANGLARGEFONT- The name of the language file you want for a “large font” display, currently only “English.”

A large text font is available on all deskphones. You can activate the larger text font only if a language file for this font is available. The **Text Size** option is presented to the user if the parameter LANGLARGEFONT is not null and if a language file for that value is used as the current user interface language. If neither condition is met, the **Text Size** option is not available to the user.

For example, if the language in use is English, and a large text font language file for English is specified in LANGLARGEFONT and available, the Text Size option is visible on the **Screen and Sounds Options** screen.

To download a language file or to review pertinent information, go to the [Avaya Support website](#).

 **Note:**

Specifying a language other than English in the configuration file has no impact on Avaya Communication Manager settings, values, or text strings.

Input methods:

If the phone does not support a character input method, use ASCII instead. The acceptable input methods are as follows:

• ASCII	• Croatian, Slovenian
• Latin-1	• Czech, Slovak
• German	• Estonian
• French	• Hungarian
• Italian	• Latvian
• Spanish	• Lithuanian
• Portuguese	• Polish
• Russian	• Romanian
• Albanian, Azeri, Turkish	• Simplified Chinese

List of languages:

- Arabic
- Dutch
- English
- French (Canada)

- French (France)
- German
- Hebrew
- Italian
- Japanese
- Korean
- Polish
- Portuguese (Brazil)
- Russian
- Simplified Chinese
- Spanish (Latin America)
- Spanish (Spain)
- Thai
- Traditional Chinese
- Turkish

Administering dialing methods

The phone has a variety of telephony-related applications that might obtain a telephone number during operation. Two dialing methods are used, depending on which version of Avaya Aura[®] Communication Manager that is running.

About internal audio parameters

The parameter AUDIOENV provides control of some internal audio parameters. Set these values only if absolutely required. In certain situations, particularly noisy environments, Avaya SSE might recommend you to change the AUDIOENV setting to reduce or eliminate the effects environmental noise can have during deskphone use.

The AUDIOENV parameter has a range of 0 to 299. The Set command:

```
SET AUDIOENV 0
```

is the nominal setting (0,0,0,0).

AUDIOENV impacts four internal variables described in the following table:

Table 14: Internal Audio Variables

Variable	Description	Possible Values
AGC_Dyn_Range	AGC dynamic range.	0 for a typical office environment (+/-9dB), 1 for +/-12dB, 2 for +/-15dB, and 3 for +/-18 AGC Dynamic range variation.
NR_thresh_Hd	The noise reduction threshold for the headset.	The noise reduction threshold for the headset has a default value of 0 for a typical office environment, 1 for call center applications, 2 and 4 for increasingly noisy audio environments, and 3 where noise reduction is disabled.
NR_thresh_Hs	The noise reduction threshold for the handset.	The noise reduction threshold for the handset has a default value of 0 for a typical office environment, 1 for call center applications, 2 and 4 for increasingly noisy audio environments, and 3 where noise reduction is disabled.
HD_Tx_Gain	Headset transmit gain.	Headset transmit gain has a default value of 0 for normal transmit gain, 1 for +6dB of gain, and 2 for -6dB of gain.

For more information, see *Audio Quality Tuning for IP Telephones, Issue 2* on www.avaya.com/support.

Managing applications on the Home screen

You can control the applications that display on the Home screen by configuring the corresponding parameters in the `46xxsettings.txt` file. The following table displays the conditions and or parameters that the deskphone requires for certain applications to be displayed on the Home screen.



Application	Parameter and value	Dependency
WML applications	<p>WMLHOME.</p> <p> Note:</p> <p>If WMLHOME is null, the deskphone screen displays <i>WML Applications Help icon</i> by default. You can suppress the display by setting WMLHELPSTAT to 0.</p>	<p>You administer the WML applications in the <code>AvayaMenuAdmin.txt</code> file.</p> <p>The deskphone displays the local WML browser only if the value of WMLHOME is not null and if you have not administered any WML applications.</p> <p>If WMLHOME is null and the value of WMLHELPSTAT is not 1, the deskphone does not display any WML items .</p>

Table continues...

Application	Parameter and value	Dependency
Settings application	N/A	The Settings application always displays unless suppressed by OPSTAT.
Greetings	N/A	<p>The Greetings program displays only if you configure the following conditions:</p> <ul style="list-style-type: none"> • AGTGREETINGSTAT has value 1, • CALLCTRSTAT has value 1, • The deskphone has a non-null call center agent ID if an agent has logged into the call center. • The Agent is not in an Available status. No Manual-In or Auto-In button has the associated LED On. • All call appearances are in the Idle state. <p> Note:</p> <p>The agent greetings can be recorded and played only by using the headset or the speaker.</p>

Related links

[WML browser properties](#) on page 184

WML browser properties

The following table shows a comparison of the WML browser properties of the deskphones:

Feature	Details
Top line	Yes
Application lines	4
Line buttons	Yes
Selectable objects per line	1
Application line height (in pixels)	31
Softkeys per screen	4
Navigation buttons	Yes
Text input	Yes
Color support	Yes

Table continues...

Feature	Details
Supported image format	JPEG
Maximum image width (in pixels)	300
Maximum image height (in pixels)	2976
Click to dial	Yes
Add to phonebook	Yes
Characters per line (normal font)	40
Characters per line (large font)	22
Characters per softkey (normal font)	8
Characters per softkey (large font)	6

Related links

[Managing applications on the Home screen](#) on page 183

Administering features on softkeys

You can administer call server features on softkeys on the phone. The number of features you can place on a set of softkeys depends on the call state the phone is presenting to the user.

The chart below lists the call states for which you can administer softkeys, the relevant system parameter associated with a call state, the maximum number of features you can specify in that system parameter, and the softkey numbers that can take administered features.

Call State	System Parameter	Maximum number of features allowed	Available Softkeys
Idle	IDLEFEATURES	6	All softkeys
Dialing	DIALFEATURES	5	1, 3, 4
Active with ringback	RINGBKFEATURES	3	3
Active with talk path	TALKFEATURES	3	4

Administration of softkeys works as follows:

- Administer feature buttons for the phone on the call server as you normally would, and the call server sends these button assignments to the phone as it always has.
- In the `46xxsettings.txt` file, administer any or all of the system parameters indicated in the chart above. Each parameter consists of a list of one or more feature numbers, up to the maximum indicated in that chart, with each feature number corresponding to a specific administrable feature.
- The phone compares the list of features administered on the call server with the list of features in the system parameters administered. If a given feature occurs both in call server administration and in a given system parameter, that feature is displayed on a phone application softkey when the highlighted call appearance is in the associated call state. The phone displays the feature buttons starting with Softkey 1 and continuing to the right in the

order specified in the system parameter, subject to the availability of features and softkeys as listed in this section.

Example:

Consider a scenario where call server administration includes the Send All Calls and Directory features. If the system parameter IDLEFEATURES is not administered, the corresponding softkeys are labeled from left to right as follows when a highlighted call appearance is Idle:

Redial	Send All	(blank)	(blank)
--------	----------	---------	---------

However, when the system parameter IDLEFEATURES is administered to be “26,1000,35” the corresponding softkeys are labeled from left to right as follows when a highlighted call appearance is Idle:

Directory	Redial	Send All	(blank)
-----------	--------	----------	---------

Softkeys available to be labeled with feature buttons as indicated under Available Softkeys in the chart are those that are not dedicated to a higher priority function. For example, in the “Active with a talk path” call state, the softkeys for Hold, Conference, and Transfer are dedicated to those functions and cannot be displaced by an administrable feature button, while the softkey normally labeled Drop (softkey #4) can be used for an administrable feature button.

In addition to the administrable feature, you can specify three additional features on a softkey of your choice or can completely replace the existing features. In the case of the system parameters IDLEFEATURES or DIALFEATURES, if the list of feature numbers includes the value 1000, the corresponding softkey is reserved for the Redial feature local to the phone. This means the corresponding softkey is labeled Redial if the phone has at least one phone number stored for the Redial feature. Otherwise the softkey is unlabeled. In the case of the system parameter IDLEFEATURES, if the list of feature numbers includes the value 1100, the corresponding softkey is reserved for a **Backlight Off** icon. When you press this softkey, the backlight of the phone turns off, saving energy. The backlight is turned on automatically when an phone activity is detected, such as an incoming call or a button press by the user.

If the list of feature numbers includes the value 1200, the corresponding softkey is reserved for a **Log Off** button, regardless of the value of OPSTAT. When pressed, this softkey presents the **Log Out Confirmation Screen**, and the user can either confirm the logout process, or cancel it and return to the Phone Screen.

For IDLEFEATURES or DIALFEATURES, if the system parameter PHNEMERGNUM is administered, the third softkey in the Idle or Dialing call state will always be labeled *Emerg* regardless of the contents of those system parameters.

Features administered only for the button module are ignored. The feature must be administered for the phone and not the button module.

Primary call appearances, bridged call appearances, and Team Buttons cannot be administered on softkeys.

The feature button softkey labels displayed to the user are those downloaded from the call server. If the user has personalized the labels, the phone displays the personalized labels.

If one of the designated parameters contains a Feature number more than once, and that number corresponds to at least one occurrence of a feature button downloaded from the call server, the designation of softkeys to features is assigned in the order the features are listed. For example, if two Abbreviated Dial (AD) buttons (Feature Number 65) are listed in the DIALFEATURES parameter, the first AD button in that list is associated with the first AD button downloaded from the call server. The second AD button in the DIALFEATURES parameter is associated with the second AD button downloaded from the call server (if any), and so on.

*** Note:**

Using the system parameters, you can specify more features than can be displayed on any one phone. For example, using the IDLEFEATURES, you can specify up to six features, although any one phone can display at most four of them. Using the maximum size of each parameter, you can specify one comprehensive list for that parameter's related call state, but allow your user community to see different feature buttons depending on how you administer their phones. Since the phone only displays feature button labels for features administered on the call server, you can set the softkey feature system parameters to values that correspond to features for some users, but not others. For example, if TALKFEATURES is administered to "325,50", the users having Conference Display administered would see that label on softkey #3 for the Active with talk path call state, but users with Attendant Release would instead see that label on softkey #3. Because softkey labels display in the order in which they are administered in the system parameter, a user with both Conference Display and Attendant Release would only see a Conference Display softkey. If the Ringer Off button is set to on, the phones will set the alert to a single short ring followed by visual ringing alerts only.

The Feature Numbers are as follows.

Table 15: CM Feature Numbers for Assigning Softkeys

Feature Name	Default Label	Feature Number
abr-prog	AbbrvDial Program	67
abr-spchar	AbbrvDial (char)	68
abrv-dial	AD	65
abrv-ring	AR	226
ac-alarm	AC Alarm	128
aca-halt	Auto-Ckt Assure	77
account	Acct	134
act-tr-grp	Cont Act	46
admin	Admin	150
after-call	After Call Work	91
alrt-agchg	Alert Agent	225
alt-frl	Alt FRL	162
ani-request	ANI Request	146
assist	Assist	90

Table continues...

Feature Name	Default Label	Feature Number
asvn-halt	asvn-halt	214
atd-qcalls	AQC	89
atd-qtime	AQT	88
audix-rec	Audix Record	301
aut-msg-wt	Message (name or ext)	70
auto-cbk	Auto Callback	33
auto-icom	Auto (name or ext)	69
auto-in	Auto In	92
auto-wkup	Auto Wakeup	27
autodial	Autodial	227
aux-work	Auxiliary Work	52
btn-ring	Button Ring	258
btn-view	Button View	151
busy-ind	Busy	39
call-disp	Make Call	16
call-fwd	Call Forwarding	74
call-park	Call Park	45
call-pkup	Call Pickup	34
callr-info	Caller Info	141
call-timer	Ctime	243
cancel	Cancel	51
cas-backup	CAS Backup	76
cdr1-alm	CDR 1 Failure	106
cdr2-alm	CDR 2 Failure	117
cfwd-bsyda	Call Forwarding bsyda (ext)	84
cfwd-enh	Call Forwarding Enhanced	304
check-in	Check In	29
check-out	Check Out	28
class-rstr	COR	59
clk-overid	Clocked Override	112
conf-dsp	Conference Display	325
con-stat	Console Status	185
consult	Consult	42
cov-cback	Coverage Callback	17
cov-msg-rt	Cover Msg Retrieve	12

Table continues...

Feature Name	Default Label	Feature Number
cpn-blk	CPN Block	164
cpn-unblk	CPN Unblock	165
crss-alert	Crisis Alert	247
cw-ringoff	CW Aud Off	62
date-time	Date Time	23
deact-tr-g	Cont Deact	47
delete-msg	Delete Message	14
dial-icom	Dial Icom	32
did-remove	DID Remove	276
did-view	DID View	256
directory	Directory	26
dir-pkup	Directory Pkup	230
disp-chrg	Display Charge	232
display	Display	180
disp-norm	Local/Normal	124
dn-dst	Do Not Disturb	99
dont-split	Don't Split	176
dtgs-stat	DTGS Status	181
ec500	Extension to Cellular	335
em-acc-att	Emerg Access to Attd	64
exclusion	Exclusion	41
ext-dn-dst	Do Not Disturb Ext.	95
extnd-call	Extend Call	345
fe-mute	Far End Mute for Conf	328
flash	Flash	110
forced-rel	Forced Release	57
goto-cover	Go To Cover	36
group-disp	Group Display	212
group-sel	Group Select	213
grp-dn-dst	Do Not Disturb Grp	96
grp-page	GrpPg	135
headset	Headset	241
hundrd-sel	Group Select #	58
hunt-ne	Hunt Group	101
in-call-id	Coverage (Info)	30

Table continues...

Feature Name	Default Label	Feature Number
in-ringoff	In Aud Off	60
inspect	Inspect Mode	21
int-aut-an	IntAutoAns	108
intrusion	Intrusion	179
last-mess	Last Message	182
last-numb	Last Number Dialed	66
last-op	Last Operation	183
lic-error	License Error	312
limit-call	LimitInCalls	302
link-alarm	Link Failure (#)	103
local-tgs	Local-tgs (#)	48
lsvn-halt	Login SVN	144
lwc-cancel	Cancel LWC	19
lwc-lock	Lock LWC	18
lwc-store	LWC	10
maid-stat	Maid Status	209
major-alm	Major Hdwe Failure	104
man-msg-wt	Msg Wait (name or ext.)	38
man-overid	Immediate Override	113
manual-in	Manual In	93
mct-act	MCT Activation	160
mct-contr	MCT Control	161
mf-da-intl	Directory Assistance	246
mf-op-intl	CO Attendant	229
mj/mn-alm	Maj/Min Hdwe Failure	82
mm-basic	MM Basic	169
mm-call	MM Call	167
mm-cfwd	MM CallFwd	244
mm-datacnf	MM Datacnf	168
mmi-cp-alm	MMI Circuit Pack Alarm	132
mm-multnbr	MM MultNbr	170
mm-pcaudio	MM PCAudio	166
msg-retr	Message Retrieve	11
mwn-act	Message Waiting Act.	97
mwn-deact	Message Waiting Deact.	98

Table continues...

Feature Name	Default Label	Feature Number
next	Next	13
night-serv	Night Serv	53
noans-alrt	RONA	192
no-hld-cnfr	No Hold Conference	337
normal	Normal Mode	15
occ-rooms	Occ-Rooms	210
off-bd-alm	Offboard Alarm	126
override	Attndt Override	178
per-COline	CO Line (#)	31
pms-alarm	PMS Failure	105
pos-avail	Position Available	54
pos-busy	Position Busy	119
post-msgs	Post Messages	336
pr-awu-alm	Auto Wakeup Alm	116
pr-pms-alm	PMS Ptr Alarm	115
pr-sys-alm	Sys Ptr Alarm	120
print-msgs	Print Msgs	71
priority	Priority	81
q-calls	NQC	87
q-time	OQT	86
release	Attendant Release	50
release	Station Release	94
remote-tgs	Remote TG (#)	78
re-ringoff	Ringer Reminder	61
ringer-off	Ringer Off	80
rs-alert	System Reset Alert	109
rsvn-halt	rsvn-halt	145
scroll	Scroll	125
send-calls	Send All Calls	35
send-term	Send All Calls-TEG	72
serial-cal	Serial Call	177
serv-obsrv	Service Observing	85
signal	Signal (name or ext.)	37
split	Split	56
split-swap	Split-swap	191

Table continues...

Feature Name	Default Label	Feature Number
ssvn-halt	ssvn-halt	231
sta-lock	Station Lock	300
start	Start Call	55
stored-num	Stored Number	22
stroke-cnt	Stroke Count (#)	129
term-x-gr	Term Grp (name or ext.)	40
toggle-swap	Conf/Trans Toggle-Swap	327
trk-ac-alm	FTC Alarm	121
trk-id	Trunk ID	63
trunk-name	Trunk Name	111
trunk-ns	Trunk Group	102
usr-addbsy	Add Busy Indicator	239
usr-rembsy	Remove busy Indicator	240
uui-info	UUI-Info	228
vc-cp-alm	VC Circuit Pack Alarm	133
verify	Verify	75
vip-chkin	VIP Check-in	277
vip-retry	VIP Retry	148
vip-wakeup	VIP Wakeup	147
vis	vis	184
voa-repeat	VOA Repeat	208
voice-mail	Message	326
vu-display	VuStats #	211
whisp-act	Whisper Page Activation	136
whisp-anbk	Answerback	137
whsp-off	Whisper Page Off	138
work-code	Work Code	140

Administering a custom screen saver

Avaya provides a standard screen saver. However, you can administer a customized screen saver for phones with bit-mapped displays. The screen saver displays when the idle timer reaches the value set in the system parameter SCREENSAVERON. The phone removes the screen saver whenever you reset the idle timer. If the value of SCREENSAVERON is "0", the phone does not display either the standard Avaya screen saver or any customized screen saver you specify in the SCREENSAVER system parameter.

The deskphones display the screen savers for approximately 5 seconds at a time at random locations on the screen, so that the entire image is always displayed. When the phone removes the screen saver, the phone restores the previously displayed screen unless a specified software operation such as making a call from the Phone screen displays some other screen.

You can administer color images for gray scale sets or black and white images for color sets. The deskphone will present the images as applicable for their displays.

To determine what image to display, the deskphone adheres to this procedure:

1. During start-up, the deskphone checks for the file named in the system parameter SCREENSAVER. If the deskphone finds a file, the deskphone checks that file for valid jpeg format, and to verify that the screen saver image height and screen saver image width do not exceed the specifications.

The screen saver should be a smaller size than these pixel values specified so the screen saver can move randomly while displaying the entire image.

2. If the deskphone does not download a valid file, either because no file exists, or because the downloaded file exceeded one or more of the pixel count limits, or because the image is not a valid JPEG image, the deskphone uses the Avaya-specific screen saver.

About 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.

Release 6.2 onwards, the IP deskphones support the ability to choose either of these standards. Because individual organizations and users differ in how they might want to implement this choice, the deskphone provides 3 ways to specify the desired audio equalization:

- **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 and 3 specifies Amplified.
- **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 `46xxsettings.txt` file, the HSEQUAL Local Procedure provides another method to administer the deskphone with the audio equalization value that you require. "Default" uses the `46xxsettings.txt` file value unless superseded by User Option. "Audio Opt." is optimized for TIA-810/920 acoustic performance, "HAC Opt." is optimized for HAC telecoil performance, and "Amplified" is optimized for setting nominal volume level between calls.
- **User Option:** The user can select "Default" by which the deskphone uses the `46xxsettings.txt` 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:
 1. The deskphone uses the User Option value if selected and saved.
 2. If a Local Procedure value was selected and saved, the deskphone uses the local Procedure value.
 3. If a settings file value is specified and saved, the deskphone uses that value.
 4. If none of the above options are set, the deskphone uses Handset equalization that is optimized for TIA-810/920 acoustic performance.

 **Note:**

The options **Default**, **Audio Opt**, **HAC Opt** and **Amplified** that are available for Handset equalization are mutually exclusive, meaning only one can be activated at a time.

About Acoustic protection

You can enable the acoustic exposure protection feature to protect the ears of the headset user. Acoustic exposure protection is supported only in L100 Series Headsets with RJ9 connector. You can configure this feature by using the `46xxsettings.txt` file or access from the phone menu **Options & Settings > Advanced Options > Acoustic Protection....**

Related links

[Acoustic protection parameter](#) on page 194

Acoustic protection parameter

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

Parameter name	Default value	Description
ACOUSTIC_EXPOSURE_PROTECT_MODE_DEFAULT	Off	Specifies the acoustic exposure protection mode. The options are: <ul style="list-style-type: none"> • Off • Dynamic • 4 hours • 8 hours

Related links

[About Acoustic protection](#) on page 194

Configuring phone based auto-answer

You can configure the auto-answer feature through the settings file now. Earlier, you could configure auto-answer through the Communication Manager only. For an incoming call, the auto-answer feature plays a zip tone to alert the agent and automatically activates the headset button and answers the call.

*** Note:**

The deskphone plays the zip tone only for the deskphone user and the caller cannot hear it, also, the phone user cannot hear any audio from the caller until the zip tone completes.

For a number having bridged call appearances, you can configure the response of the auto-answer feature for an incoming call based on settings for new parameters AUTOANSSTAT and AUTOANSSTRING. You can also specify whether the deskphone will alert audibly with auto-answering calls using AUTOANSALERT.

You can also configure auto-answer for the incoming call, based on the numbers having a fixed VDN name. You can configure auto-answer not to occur for calls arriving from unidentified numbers or DIDs.

You can configure these parameters in the `46xxsettings.txt` file.

AUTOANSSTAT

Parameter name and default value: AUTOANSSTAT ('0')

Valid values: 1 ASCII numeric digit, '0' through '4'

Usage: Specifies whether the deskphone will auto-answer incoming calls or not.

*** Note:**

AUTOANSSTAT is independent of any call center parameter or status, it functions regardless of whether an agent is logged in or not.

AUTOANSSTRING

Parameter Name and (default value): AUTOANSSTRING("")

Valid Values: 0-15 ASCII characters

Usage: Specifies the name that must match with the incoming VDN name to auto-answer. The incoming VDN name can be longer but the vector matches only the first 15 characters.

AUTOANSALERT

Parameter Name and (default value): AUTOANSALERT ('0')

Valid Values: 1 ASCII numeric digit, '0' and '1'

Usage: Specifies whether the deskphone will audibly alert with auto-answering calls.

*** Note:**

If AUTOANSALERT is 0, the deskphone will not provide audible alerting when auto-answering a call, regardless of any other setting (e.g. AUDASYS). Similarly if AUTOANSALERT is 1, the

deskphone will provide audible alerting when auto-answering a call, if and only if the phone is administered to provide audible alerting at all, for example by user Volume setting.

Scenarios addressed using the parameters

You can configure these parameters to address the following scenarios for an incoming call on primary appearance A and a bridged appearance B:

*** Note:**

To avoid conflicts when using Phone-based conditional auto-answer, configure auto-answer settings on CM to none.

Table 16: Parameter values and results

Value of AUTOANSSTAT	Value of AUTOANSSTRING	Resulting scenario
0	Specified or null value	The deskphones do not auto-answer the call.
1	Null	Auto-answer is attempted on both primary and bridged call appearances (BCAs), and CM will adjudicate any race condition.
1	Specified and matches the VDN	Auto-answer is attempted on both primary call appearances (PCAs) and BCAs, and CM will adjudicate any race condition.
1	Specified but does not match VDN	No auto-answer on either PCAs or BCAs.
2	Null	Auto-answer is attempted on PCAs but not BCAs
2	Specified and matches the VDN	Auto-answer is attempted on PCAs but not BCAs.
2	Specified and does not match VDN	No auto-answer on either PCAs or BCAs.
3	Not specified	Auto-answer is attempted on both PCAs or BCAs only for deskphones used by an agent logged into a call center (regardless of status such as Ready, Aux Work, etc.
3	Specified and matches VDN	Auto-answer is attempted on both PCAs or BCAs only for deskphones used by an agent logged into a call center (regardless of status such as Ready, Aux Work, etc.)

Table continues...

Value of AUTOANSSTAT	Value of AUTOANSSTRING	Resulting scenario
3	Specified and does not match VDN	No auto-answer on either PCAs or BCAs.
4	Not specified	Auto-answer is attempted on PCAs only and only for deskphones used by an agent logged into a call center (regardless of status such as Ready, Aux Work, etc.)
4	Specified and matches VDN	Auto-answer is attempted on PCAs only and only for deskphones used by an agent logged into a call center (regardless of status such as Ready, Aux Work, etc.)
4	Specified and does not match VDN	No auto-answer on either PCAs or BCAs.

*** Note:**

To prevent the condition where both a primary and bridged call appearance (on two separate deskphones) auto-answer an incoming call, you should use either of the following approaches, as applicable to your environment:

- Put the deskphones that you want to auto-answer in a GROUP with AUTOANSSTAT set to 1 (or any other applicable value), and put the other deskphones in a different GROUP with AUTOANSSTAT set to 0. The first Group will auto-answer the call as applicable, and the second Group will never auto-answer the call.
- Set AUTOANSSTAT to 2 for all deskphones so that only the primary call appearances auto-answer calls.

Administering backup and restore

The phone supports the HTTP client to back up and restore the user-specific data. HTTP over TLS (HTTPS) is also supported for backup or restore. For backup, the deskphone creates a file with all the user-specific data if a backup file location is specified in system parameter BRURI. The file is sent to the server by an HTTP PUT message, with appropriate success or failure confirmation.

*** Note:**

IP phone H.323 v6.6.2 and later do not support HTTPS with MV_IPTTEL or IIS 6. It is recommended to upgrade to the current version of an HTTPS server that supports TLS 1.2.

For restore, the initiating process must supply only the backup file name. The file is requested from the server by an HTTP GET message. If successful, the file is returned to the initiating process. Otherwise a failure message is returned.

Backup and restore operations construct the URI used in the HTTP message from the value of the BRURI parameter and from the file name as follows:

- If BRURI ends with a / (a forward slash), the file name is appended.
- Otherwise, a forward slash and the file name is appended to the BRURI value.

 **Note:**

BRURI can include a directory path and/or a port number as specified in IETF RFCs 2396 and 3986.

If you use TLS, the call server registration password for the phone must be included in an Authorization request-header in each transmitted GET and PUT method. This is intended for use by the Avaya IP Telephone File Server Application (which can be downloaded from the Avaya support Web site) so that the phone requesting the file transaction can be authenticated.

If no digital certificates are downloaded based on the system parameter TRUSTCERTS, the phone establishes a TLS connection only to a backup/restore file server that has a Avaya-signed certificate, included by default with the Avaya IP Telephone File Server Application, and includes the credentials. However, if at least one digital certificate has been downloaded based on TRUSTCERTS, the credentials are included only if BRAUTH is set to 1. This is a security feature to allow control over whether the credentials are sent to servers with third-party certificates. If the server on which the Avaya IP Deskphone File Server Application is installed uses a non-Avaya certificate, set BRAUTH to 1 to enable authentication of the deskphones. The default value of BRAUTH is 0.

When the call server IP address and the registration password of the phone are included as the credentials in an Authorization request-header, the call server IP address is included first in dotted-decimal format, followed by a colon, hex 3A, followed by the registration password of the phone.

HTTP/HTTPS authentication is supported for both backup and restore operations. The authentication credentials and realm are stored in re-programmable, non-volatile memory, which is not overwritten when new phone software is downloaded. Both the authentication credentials and realm have a default value of null, set at manufacture or at any other time user-specific data is removed from the phone.

The following cipher suites are supported for backup and restore operations:

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS 1.2

If the digital certificate of the server is signed by the Avaya Product Root Certificate Authority certificate, the call server registration password of the phone is included as the credentials in an Authorization request-header for each transmitted PUT (backup) and GET (for restore) method.

New values replace the currently stored authentication and realm values:

- When HTTP authentication for backup or restore succeeds and
- If the userid, password, or realm used differs from those currently stored in the phone

If HTTP authentication fails, the user is prompted to enter new credentials.

*** Note:**

Users can request a backup or restore using the Advanced Options Backup/Restore screen, as described in the user guide for their specific deskphone model.

Related links

[Backup file formats](#) on page 199

[User data saved during backup](#) on page 200

[About restore](#) on page 201

Backup file formats

When the system parameter BRURI is non-null, user changes are automatically backed up to the file `ext_96xxdata.txt` (where `ext` is the extension number of the deskphone) on the HTTP server to a user-specified folder. The backup formats are as follows:

Table 17: Backup File Formats

Item/Data Value	Format
Generic	<i>name=value</i>
Contacts	ABKNAMEmmm=ENTRY_NAME ABKNUMBERmmm=ENTRY_NUMBER_1 ABKTYPEmmm=ENTRYT_TYPE (where <i>mmm</i> is the one-, two-, or three-digit entry ID, with leading zeros for single and double-digit entry IDs)
Call Log entries	CLNAMEmmm=ENTRY_NAME CLNUMBERmmm=ENTRY_NUMBER CLTYPEmmm=ENTRY_TYPE CLDATEmmm=ENTRY_DATE CLTIMEmmm=ENTRY_TIME CLDURATIONmmm=ENTRY_DURATION CLBRIDGEDFLAGmmm=ENTRY_BRIDGEDFLAG CLMISSEDCNTRmmm=ENTRY_COUNTER CLBCALBLmmm=ENTRY_BCALBL To be valid, a Call Log entry must have at least a non-null Date and Type, and either Name or Number or both must be non-null.

Table continues...

Item/Data Value	Format
User-generated Call Appearance labels with button identifiers of <i>mm</i> where <i>mm</i> is the one- or two-digit button number of the entry with a lead zero for single-digit numbers.	PHNLABEL <i>mm</i> =CAUSERLABEL
User-generated deskphone feature labels with button identifiers of <i>mm</i> , where <i>mm</i> is the one- or two-digit button number of the entry with a lead zero for single-digit numbers.	PHNLABEL <i>mm</i> =FBUSERLABEL
User-generated button module call appearance or feature labels with button identifiers of <i>mm</i> , where <i>mm</i> is the one- or two-digit button number of the entry with a lead zero for single-digit numbers.	SBMLABEL <i>mm</i> =CAUSERLABEL or FBUSERLABEL, as applicable

Related links

[Administering backup and restore](#) on page 197

User data saved during backup

A backup saves the options and non-password parameters. The parameter and the applicable settings are shown in the following table.

Table 18: Options and non-password parameters saved during backup

Parameter Name	Setting
HEADSETBIDIR	Full support of wireless headset that includes on/off-hook control
USER_HSEQUAL	User-specified handset audio equalization standard
LANGUSER	Display Language
LOGACTIVE	Call Log Active
LOGBRIDGED	Log Bridged Calls
LOGTDFORMAT	Call Log Data Time/Date Format
OPTAGCHAND	Handset Automatic Gain Control
OPTAGCHEAD	Headset Automatic Gain Control
OPTAGCSPKR	Speaker Automatic Gain Control
OPTAUDIOPATH	Audio Path
OPTCLICKS	Button Clicks
OPTERRORTONE	Error Tones
OPTGUESTLOGIN	Guest Login Permitted/Not Permitted
OPTTEXTSIZE	Text Size

Table continues...

Parameter Name	Setting
PERSONALRING	Personalized Ring. Note: This value is backed up as equal to the PERSONALWAV value when PERSONALWAV is set to one of the 8 standard ring patterns. When PERSONALWAV is greater than 8 (meaning it is set to one of the newer ring patterns) and PERSONALRING was set using a backup file value, that backup value is re-saved. If neither of these conditions apply, no PERSONALRING value is backed up.
PERSONALWAV	Personalized Ring value
PHNABKNAME	Contacts Pairing
PHNEDITDIAL	Edit Dialling
PHNRDIAL	Redial
PHNSCRONANS	Go to Phone Screen on Answer
PHNSCRONCALL	Go to Phone Screen on Calling
PHNSCRONALERT	Go to Phone Screen on Ringing
PHNSCRWIDTH	Phone screen width
PHNTIMERS	Call Timer
PHNVISUALALERT	Visual Alerting
PRINGMENU	Personalized Ring Menu

Related links

[Administering backup and restore](#) on page 197

About restore

When automatic or user-requested retrieval of backup data is initiated, user data and settings are set to the values contained in the backup file. The user-requested retrieval of backup data occurs only if the OPSTAT parameter setting allows the user to change those values. Therefore, any restrictions set using OPSTAT are given priority and implemented.

The backup file value is not retrieved, and the current setting remains valid:

- When a value in the backup file has changed and
- That value corresponds to an application that OPSTAT indicates should not be changed.

This method prevents a user from bypassing the administration of OPSTAT and changing settings in the backup file.

*** Note:**

If you administered the OPSTAT parameter to suppress changes to one or more applications, the phone backs up and restores data as usual, but ignores data for “suppressed” applications. This method prevents a user from bypassing your OPSTAT restrictions by editing the backup file.

During backup file restoration, do not perform any user activity until the phone displays a `Retrieval successful` or `Retrieval Failed` .

When a restore attempt fails, if a retrieved file has no valid data, or if a retrieved file cannot be successfully stored, the phone displays a `Retrieval Failed` message until the user takes another action.

Important considerations during data retrieval are as follows:

- When you create a backup file instead of editing an existing one, ensure to create the file with UTF-16 LE (little endian) characters, with Byte Order Mark (BOM) for LE of 0xFFFE.
- Backup saves data values using the generic format *name=value*.
- All identifiers, for example, *names*, are interpreted in a case-insensitive manner, except parameter values, Contact names, and numbers.
- Spaces preceding, within, or following a *name* are treated as part of the *name*.
- <CR> and <LF> (UTF-16 characters 0x000D and 0x000A, respectively) are interpreted as line termination characters.
- Blank lines are ignored.
- When an identifier is not recognized or is invalid, the entire line is ignored. Similarly, if an identifier is valid but the data itself is invalid or incomplete, the line is ignored.
- When an identifier is valid with valid and complete data, but the data is not applicable to the current state of the phone, the data is retained for possible use later, and is treated as data to be backed up at the appropriate time.

For example, if labels for a button module are present, but no such module is attached to the deskphone, the button labels are retained.

- When more than one line contains a value for an option, parameter, or Contacts entry, the last value read is retrieved, to allow new values to overwrite previous values as lines are read from the backup file. In all other cases, the line order in the backup file has no bearing on retrieval.
- The existence of invalid data does not constitute a failed retrieval. The success of the retrieval process requires the phone to get the backup file and successfully restore valid data.

Related links

[Administering backup and restore](#) on page 197

Administering Applications and Options

Avaya IP Phone includes various application settings that you must configure to activate an application for end users.

Customizing Applications and Options

The phone has some unique and powerful capabilities that take advantage of the display and access to LAN facilities. For example, if your LAN has a WML Web site, the phone needs key information about the servers providing those facilities. You must provide the information in the file, depending on the applications you want to make available to your end users.

Caution:

For a phone to work properly, you must have the `46xxsettings.txt` file in the same directory as the application file. If you do not edit the `46xxsettings.txt` file, those deskphones use default settings only. The `46xxsettings.txt` file is available as a standalone download. If you already have such a file because you downloaded it for a previous release, installing the standalone file overwrites the original file.

Note:

To facilitate administration, use the `46xxsettings.txt` file.

The following is a list of applications or functions and the parameters that apply to those applications. Parameters shown as Mandatory must be accurate and non-null for the application to work; other parameters listed are optional. You can change parameters to suit your environment. If you do not include these parameters in the settings file, the default values are used.

Backup/restore parameter - BRURI (Mandatory)

Backlight parameter - BAKLIGHTOFF

Call log/history parameters - CLDELCALLBK, LOGBACKUP, LOGMISSEDONCE, LOGUNSEEN

General user parameters - APPSTAT, OPSTAT, OPSTAT2

Guest login parameters - GUESTDURATION, GUESTLOGINSTAT, GUESTWARNING

Options parameter - RINGTONESTYLE

Phone parameter - FBONCASCREEEN

User Timer (Stopwatch) — TIMERSTAT

VPN parameters - VPN parameters. For more information on VPN parameters, see *VPN Setup Guide for 9600 Series IP Telephones*.

Web access application parameters - SUBSCRIBELIST, TPSLIST, WMLEXCEPT, WMLHELPSTAT, WMLHOME (Mandatory), WMLIDLETIME, WMLIDLEURI, WMLPORT, WMLPROXY, WMLSMALL.

Setting the Application Status flag

the phone offer numerous applications like Contacts, Call Log/History, Redial, and so on to the users. Each of these applications allows the user to add, delete, or in some cases, edit entries.

You, as the administrator, might not want the user to use that level of functionality. For example, a user cannot delete the contact number of the concierge from the hotel lobby deskphone. Further, for privacy reasons, that same deskphone must display the Call Log. You can use the Application Status Flag, APPSTAT, to administer specific application functionality permission levels for one or more deskphones.

APPSTAT consists of one number, specifying a certain level of allowed functionality. A Zero, 0, value provides no functionality. Values 2 and 3 provide increasing levels of functionality, and value 1 provides the user complete application functionality.

Table 19: Application status flags and their meaning

APPSTAT value	Meaning
0	Redial and Call Logs/History are suppressed. The user cannot change Contacts.
1	All administered applications are displayed, with full functionality. This is the default value.
2	Call Log (History) is suppressed. Contact changes are not allowed. Only one-number Redial is allowed.
3	Contact changes are not allowed.

Suppressed applications are not displayed to the user. Softkey labels and application tabs are not labeled or displayed. The deskphones continue to display options associated with suppressed applications unless you override them by appropriate OPSTAT parameter administration. Displayed options have no effect while the application is suppressed. The message *Contact changes are not allowed* means the Contacts application displays and the user can make calls as normal. The deskphone does not display any controls using which the user can change any aspect of the Contact application including adding, deleting, or editing any Contact name or number. This restriction includes the ability to add, delete, or edit any Contact name or number. The message *Only one-number Redial is allowed* means the user option that allows a choice between displaying last numbers dialed is suppressed. The Redial buffer stores only one number. The deskphone does not display the Redial application as the user can redial only one number. This restriction allows privacy once a given user has left the deskphone.

You can:

- Set APPSTAT to 1, for example, in a staging area
- Administer a given deskphone with Contact entries of your choice, like the Concierge deskphone number button in the earlier example
- Then move the deskphone to where it will be used, where you have administered APPSTAT to be, for example, 0

When you change the location of the deskphone and the relocated deskphone resets, it retains its Contact entries, like Concierge, but does not allow the user to create new entries.

When you set APPSTAT to any valid value other than 1, the deskphone does not accept any Contact button label changes that might have been made directly on a backup file. Only the existing labels of the deskphone are used. This restriction prevents circumvention of the APPSTAT restrictions.

The WML applications are also suppressed by default.

Administering the Avaya menu

The Main menu is a list of sub-applications the user can select from to invoke the corresponding functionality. A file called *AvayaMenuAdmin.txt* is available with downloads on which you can specify the menu label, URI, and list order of WML applications on the Avaya menu.

! Important:

You must set the system parameter AMADMIN in the `46xxsettings.txt` file for Avaya menu to work with WML applications.

If WML applications are installed and the system parameter AMADMIN is set in the `46xxsettings.txt` file:

- The WML applications appear in the first-level Avaya menu.
- The first level Avaya menu includes a single entry (Phone Settings) that leads to a screen containing choices for Options & Settings and Network Information.
- The Phone Settings screen is essentially the current Options and Settings menu, with the addition of Network Information.

If WML applications are installed and the system parameter WMLHOME is set in the `46xxsettings.txt` file, the Avaya menu is identical.

If WML applications are not installed, the Avaya menu is the same as the current **Options & Settings** menu, with the addition of **Network Information**, **VPN Settings**, **Log Off**, and **About Avaya IP Deskphone**.

Depending on how you have administered WML applications, you can present the alternatives for sub-applications as follows:

- Set the system parameter AMADMIN to the URL of the *AvayaMenuAdmin.txt* in the `46xxsettings.txt` file when you want to display multiple WML applications on the Avaya menu.
- Set the system parameter WMLHOME in the `46xxsettings.txt` file for all except the 9610 when you want the deskphone to display the Browser instead of individual applications.
- Take no action to administer WML applications.
- The Browser application is listed only if it is properly administered. Administration also includes a non-null value for WMLHOME.

Sample Avaya Menu Administration File Template

```
#####
## ## AVAYA MENU CONFIGURATION FILE TEMPLATE ##
```

```
#####

## This file is to be used as a template for configuring the ##Avaya
Main Menu. See the Avaya IP Deskphone H.323 ##Administrator Guide for
details. Both are available on ##support.avaya.com ##

##Since the AMICON parameter applies only to touch screen phones, it is
not shown in the sample below.

#####

##

## AMLBLxx=Label up to 16 unicode characters
## AMTYPExx=Type 1=WML-Application; 2=local Phone Settings
## 3=local LogOff Application;4=local About Avaya Screen
## 5=Guest Login; 6=My Pictures
## AMDATAxx URI of up to 255 ASCII-characters e.g. http://yy.yy.yy.yy/
*.wml

## The tags AMLBLxx and AMDATAxx are only used if AMTYPExx = 1
## Multiple definitions of local applications (Type 2.4)
## will be suppressed. The last tag is valid.
## xx describes the sequence in the Avaya Menu and is valid
## from 01 to 12.

##

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

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

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

##AMTYPE04=
##AMLBL04=
##AMDATA04=
```

```
##  
##AMTYPE05=  
##AMLBL05=  
##AMDATA05=  
##  
##AMTYPE06=  
##AMLBL06=  
##AMDATA06=  
##  
##AMTYPE07=  
##AMLBL07=  
##AMDATA07=  
##  
##AMTYPE08=  
##AMLBL08=  
##AMDATA08=  
##AMTYPE09=  
##AMLBL09=  
##AMDATA09=  
##  
##AMTYPE10=  
##AMLBL10=  
##AMDATA10=  
##  
##AMTYPE11=  
##AMLBL11=  
##AMDATA11=  
##  
##AMTYPE12=  
##AMLBL12=  
##AMDATA12=
```

Administering guest users

About this task

A guest user is a person who logs into a phone other than the primary phone at the home location of the user.

The guest user can log in to a phone that is across the country from the home location or one in the office near home office. You administer permission for guest login by setting the system parameter GUESTLOGINSTAT to 1 (permitted), that displays the Guest Login option on the Avaya "A" Menu.

Other related parameters that you can administer are GUESTDURATION and GUESTWARNING.

Administering visiting users

About this task

A visiting user is anyone who uses a IP deskphone in one location, for example, New York, and intends to register to a call server in some other location. For example in Paris. Typically, this occurs when a user has travelled from his/her home location to another location in the organization, but wants to register with the call server back home. The user might want to get the specific administered feature buttons, etc. provided by the home call server.

To allow this functionality, the parameter VUMCIPADD should be administered in the 46xxsettings.txt file at the current location for the visitor, with the IP addresses of their home call servers. From then on, the deskphone operates as specified in [Registration with the call server](#) on page 77.

Idle timer configuration

When the idle timer in the deskphone expires, you can administer the deskphone to turn the backlight to the lowest power level, put up a screen saver, or show a Web page while the deskphone is idle. However, do not set all these values on the same deskphone. However, you can set a lobby phone to go to a Web page when the phone is idle. You can also set a desk phone to go to the screen saver or set the backlight to low power mode when idle.

The related system parameters and their default values are:

System parameter	Default value
WMLIDLETIME	10 minutes
WMLIDLEURI	Null
BAKLIGHTOFF	120 minutes
SCREENSAVERON	240 minutes

You must specify WMLIDLEURI only for phones installed in public areas through the use of a GROUP parameter.

Table 20: Idle Timer Settings and Results

Shortest Timer	Middle Timer	Longest Timer	Operation
WMLIDLETIME and WMLIDLEURI are null	BAKLIGHTOFF is non-zero	SCREENSAVERON is non-zero	Default operation: After BAKLIGHTOFF minutes, the backlight is set to low power mode. After (SCREENSAVERON – BAKLIGHTOFF) additional minutes, the screen saver is displayed. WMLIDLETIME has no effect.
WMLIDLETIME and WMLIDLEURI are null	SCREENSAVERON is non-zero	BAKLIGHTOFF is non-zero	After SCREENSAVERON minutes, the phone displays the screen saver. After (BAKLIGHTOFF-SCREENSAVERON) additional minutes, the backlight is set to low power mode.
WMLIDLETIME and WMLIDLEURI are non-null	BAKLIGHTOFF is non-zero	SCREENSAVERON is non-zero	Every WMLIDLETIME minutes, a GET is sent for WMLIDLEURI, and the the phone displays a browser. The Web page may contain a timer to cycle through additional Web pages. The backlight is set to low power mode after the specified time and the phone displays a screen saver on the SCREENSAVERON value.

*** Note:**

You can administer the Backlight Off icon on a IP deskphone softkey.

The behavior of backlight for any adjunct button module depends on the backlight of the phone to which you attach the button module.

Chapter 5: Administration overview and requirements

Parameter data precedence

If you administer a parameter in multiple places, the last server to provide the parameter takes precedence. The following is a list of precedence, from lowest to highest:

1. Manual administration. Call server or HTTP server or both are two exceptions for the phone parameter STATIC.
2. DHCP, except as indicated in “DHCPACK Setting of Parameter Values” in [Setting up the DHCP server](#) on page 109.
3. The `46xxsettings.txt` file.
4. The Avaya call server.
5. Backup files, if administered and permitted.
6. LLDP: Only the IPv4 mode supports LLDP.

 **Note:**

Setting the call server and file server IP addresses have the lowest precedence.

Related links

[Administrative requirements](#) on page 73

Initialization process overview

The deskphone initialization process includes exchange of information that happens when the phone initializes and registers. The process includes the following five steps.

You must administer all equipment properly prior to initialization.

 **Note:**

When you start a deskphone without access to the HTTP server, the phone reuses parameters from before the reboot. The phone waits for 60 seconds and starts with the old parameters.

Related links

[Administrative requirements](#) on page 73
[Connection to network](#) on page 75
[DHCP processing](#) on page 75
[File downloads](#) on page 75
[Certificates usage](#) on page 76
[Registration with the call server](#) on page 77
[Connection to network](#) on page 75
[DHCP processing](#) on page 75
[File downloads](#) on page 75
[Certificates usage](#) on page 76
[Registration with the call server](#) on page 77

Connection to network

The phone is appropriately installed and powered. After a short initialization process, the phone displays the speed at which it is connected to the network and determines whether to initiate 802.1X network access procedures.

Related links

[Initialization process overview](#) on page 74
[Initialization process overview](#) on page 74

DHCP processing

If an IP address has not been manually configured in the phone, the phone initiates DHCP. Among other data passed to the phone is the IP address of the HTTP or HTTPS server.

Related links

[Initialization process overview](#) on page 74
[Initialization process overview](#) on page 74

File downloads

Avaya phone uses the HTTP server to download software. The HTTPS server is used to download upgrade file, configuration files, language files, certificate files and to backup or restore user information.

The phone first downloads the upgrade file to identify the latest software files. Then, the phone downloads the settings file to identify the required language files and/or certificate files. Finally, the phone downloads software files depending on the software of the phone and if it is the same as that specified in the upgrade file.

 **Note:**

HTTPS can be used to download configuration files only. Software files are downloaded using HTTP only (no HTTPS file download is supported). Configuration files can be downloaded using HTTP or HTTPS.

Related links

[Initialization process overview](#) on page 74

[Initialization process overview](#) on page 74

Certificates usage

The H.323-based phones use certificates to verify the authenticity of the following:

- HTTPS file server for downloaded configuration files, and user backup and restore files.
- H.323 signaling over TLS.
- VPN, when certificate authentication method is used.
- SLAMon server.
- SSO applications.
- 802.1x EAP-TLS.

Related links

[Initialization process overview](#) on page 74

[Certificate revocation](#) on page 76

[Initialization process overview](#) on page 74

[Certificate revocation](#) on page 76

Certificate revocation

The certificates are published by the certificate authority with information about the revocation status. The deskphones use Online Certificate Status Protocol (OCSP) to verify the revocation status of all the certificates in the chain between the server certificate and the root certificate. The root certificate is not verified. The revocation check of the certificates is done by sending HTTP or HTTPS requests to the OCSP server.

The certificates may or may not include the authority information access (AIA) extension.

The OCSP responder follows RFC 2560. The deskphones accept only signed responses. The validation of the signed response is done by using one of the three options mentioned in section 4.2.2.2 in the RFC:

1. The OCSP response is signed using CA which is trusted certificate is administered using OCSP_TRUSTCERTS.
2. The OCSP response is signed using CA which is also used to sign the certificate in question.

3. The OCSP response is signed using CA which includes a value of id-kp-OCSPSigning in an ExtendedKeyUsage extension and is issued by the CA that issued the certificate in question.

The following `46xxsettings.txt` file parameters are used by OCSP for certificate revocation:

- OCSP_ENABLED
- OCSP_URI
- OCSP_URI_PREF
- OCSP_ACCEPT_UNK
- OCSP_NONCE
- SERVER_CERT_RECHECK_HOURS
- OCSP_TRUSTCERTS

Related links

[Certificates usage](#) on page 76

[Certificates usage](#) on page 76

Registration with the call server

The call server referred to in this section is Avaya Aura[®] Communication Manager.

The phone is registered with the call server in two modes, named registration and unnamed registration.

Named registration

In this step, the phone might prompt the user for an extension and password. The phone uses that information to exchange a series of messages with the call server. For a new installation and for full service, the user can enter the phone extension and the password configured on the call server for that particular extension. The information required to restart a phone that was previously registered with an extension number is already stored on the phone. The user must confirm the information so that the phone is appropriately registered and can download call server data such as feature button assignments.

Unnamed registration

Unnamed registration provides the telephone with a restricted class of service, such as emergency calls, if administered on the call server. Using this feature, you can register a deskphone with the call server without an extension. To invoke Unnamed Registration, either enter a null (empty) extension or password or take no action. Unnamed registration is controlled on both the Communication Manager and the UNNAMEDSTAT parameter in the `46xxsettings.txt` file.

The UNNAMEDSTAT specifies whether unnamed registration is initiated by the deskphone, if a value is not entered at the extension registration prompt within 60 seconds. Valid values for this parameter are:

- 0: Disabled

- 1: Enabled

You can choose to take no action and allow the “Extension...” prompt to display for 60 seconds. The phone automatically attempts to register by means of Unnamed Registration.

A phone registered with Unnamed Registration has the following characteristics:

- Only one call appearance
- No administrable features
- Outgoing calls only, subject to call server Class of Restriction or Class of Service limitations
- Conversion to normal named registration possible by the user entering a valid extension and password.

Related links

[Initialization process overview](#) on page 74

[Other administrable options using parameters](#) on page 78

[Initialization process overview](#) on page 74

[Other administrable options using parameters](#) on page 78

Other administrable options using parameters

- MCIPADD

You can configure the phone to register to a particular call server by listing the IP addresses in the MCIPADD parameter in DHCP or the `46xxsettings.txt` file. The standard practice is to list the CLANs on the main call server, followed by any Enterprise Survivable Server (ESS) addresses, followed by any Local Spare Processor (LSP). To deviate from this practice, you can list CLANs for multiple main call servers. In general, the phone will start from the beginning of MCIPADD and attempt to register with each IP address in turn, one at a time, until the phone gets a positive response. If MCIPADD is administered, users can register to local call servers.

- VUMCIPADD

Visiting User (VU) registration is when a user from another location wants to register with their home call server using their home extension. The phone support VU registration by using the VUMCIPADD parameter.

When this parameter contains one or more IP addresses, the user sees a slight change to the Login screen. In that screen the user is asked to specify a Login Mode of either Default or Visiting User. If the user selects Default, the deskphone uses the MCIPADD parameter value whereas if the user selects Visiting User, the deskphone attempts to register with each IP address in VUMCIPADD simultaneously until it gets a positive response.

Note:

Only the Challenge and Annex-H profiles are supported in the VU mode.

For example, if the company has locations in cities A, B, C, and D, you can administer VUMCIPADD with one IP address from each of the main call servers in the four cities. A user from city A is in the city B location but wants to use the city A call server. The user selects

Visiting User on the Login screen, the deskphone contacts each of the four main call servers simultaneously and registers with the only call server that gives a positive response for city A.

- **UNNAMEDSTAT**

Specifies whether unnamed registration is initiated by the deskphone, if a value is not entered at the extension registration prompt within 60 seconds. Valid values for this parameter are:

- 0: Disabled
- 1: Enabled

Related links

[Registration with the call server](#) on page 77

[Registration with the call server](#) on page 77

JITC security compliance mode overview

The Avaya phone H.323 firmware Release 6.8 adheres to the Joint Interoperability Test Command (JITC) security compliance requirements. According to the US Department of Defense guidelines summarized in the UCR document, these security features must be supported by the setup. These features were tested by JITC.

Avaya Aura® Communication Manager 6.3.6 and later support the JITC security compliance mode. In the JITC security compliance mode, Communication Manager and the deskphones communicate using the certified algorithms of Federal Information Processing Standards 140-2.

Supported features

The following features are supported in the JITC security compliance mode:

- Random number generator PRNG [SP 800-90] DRBG using CTR DRBG (AES-256), with deviation function enabled
- H.323 signaling over TLS or Annex-H
- SRTP using 1-serp-aescm128-hmac80 cipher suite
- Image, settings files, or certificates download over HTTP or HTTPS
- Backup and restore configuration files
- PKCS12 file generated in FIPS mode
- OCSP
- LLDP
- SNMPv2c
- Syslog
- Call center environment including Agent Greeting files

The following features are not supported in the JITC security compliance mode:

- SSH server
- IPsec VPN tunnels
- Visiting users
- SLA Monitor
- Push server
- WML browser
- SSO
- 802.1x EAP-TLS
- SCEP

 **Note:**

H.323 signaling over TLS is supported in both FIPS and non-FIPS mode.

Related links

[Administrative requirements](#) on page 73

[JITC security compliance mode configuration](#) on page 80

[JITC security compliance mode configuration](#) on page 80

JITC security compliance mode configuration

You must configure the deskphone to work in the security mode in which the UCR requirements to the JITC test cases are complied. In the `46xxsettings.txt` file, set the parameters to the values specified in the table below.

Parameter	Value	Description
FIPS_ENABLED	1	Use cryptographic algorithms using embedded FIPS 140-2-validated cryptographic module.
PROCSTAT	0	Enables local CRAFT procedure.

Table continues...


Parameter	Value	Description
PROCPSWD	Obtained from Communication Manager, DHCP server, or file server	<p>Restricts the use of the default administration password of the deskphone. The value can be set on Communication Manager, DHCP server, or file server.</p> <p> Note:</p> <p>Obtaining PROCPSWD through Communication Manager is the most secure method. Setting PROCPSWD using HTTPS is secure only if mutual certificate authentication is done.</p>
PKCS12URL	URL of the PKCS #12 file	The PKCS #12 file contains an identity certificate for the deskphone, and the corresponding private key. After the file is downloaded by the phone, the user is required to enter the password.
TRUSTCERTS	List of trusted certificate files	Trust certificates are used as trust points for TLS connections.
TLSSRVERVERIFYID	1	To verify the identity of the TLS server against the identity in the certificate. The identity of server as presented in subject common name or subjectAltName is compared with the relevant IP address or host name of the server. The server is configured using BRURI for Backup/restore over HTTPS, TLSSRV for HTTPS file server for configuration files download, and MCIPADD for H.323 over TLS signaling.
OCSP_ACCEPT_UNK	1	Specifies whether a certificate is authenticated even if its revocation status cannot be determined. Valid values are: 0 to 1.

Table continues...


Parameter	Value	Description
OCSP_ENABLED	1	<p>Specifies whether OCSP is used to verify the revocation status of the certificates.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • 0: OCSP is not used. • 1: OCSP is used to check the revocation status for the certificates presented by peers for any TLS connection. For example, HTTPS, 802.1x with EAP-TLS, SLA Mon agent, IPsec VPN, or SSO. <p> Note:</p> <p>H.323 over TLS, Backup/restore, and file downloads are the only applications supported in the secured mode. 802.1x EAP-TLS, SLA Mon, IPsec, VPN, and SSO are not supported.</p>
OCSP_URI_PREF	1	<p>OCSP responder URI can either be obtained from the certificate presented by the server, or can be locally configured on the phone in OCSP_URI.</p> <p>OCSP_URI_PREF specifies the preference between the two sources.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> • 1: OCSP_URI_PREF is used first and then the value from the OCSP field of the Authority Information Access (AIA) extension of the certificate is checked. • 2: OCSP field of the Authority Information Access (AIA) extension of the certificate is checked first and then OCSP_URI_PREF is used.
OCSP_URI	URI of the OCSP responder	<p>Specifies a URI for an OCSP responder. The URI can be an IP address or a host name.</p>

Table continues...


Parameter	Value	Description
OCSP_NONCE	1	Specifies whether a nonce is included in OCSP requests and expected in OCSP responses. Valid values are: 0 or 1.
OCSP_TRUSTCERTS	List of the trusted OCSP certificate files	Specifies the list of the trusted OCSP certificates to be downloaded. Acts as a separate trusted certificate repository for the OCSP Trusted Responder Model and contains certificates to be trusted by the OCSP responder. Local OCSP trusted certificates are used for cases where the OCSP responder certificate is signed by a CA that is different from the one used to sign the server certificate.
TLS_SECURE_RENEG	1	Specifies whether a TLS session should be terminated if the peer does not support secure renegotiation. Valid values are 0 or 1.
HTTPSRVR	IP address of the HTTP server	Used to download only the firmware files by HTTP.
TLSSRV	IP address of the HTTPS server	Used to download the configuration files by using HTTPS.
AUTH	1	Used to enforce download of configuration files using HTTPS only.  Note: If AUTH is set to 1, and the trusted certificate repository is not null, the phone will only download configuration files from HTTPS that has a certificate signed by CA. The root certificate of this CA must be in the trusted certificate repository.
OPSTAT	101	Restricts displaying the configuration information on the deskphone.

Table continues...

Parameter	Value	Description
SNMPSTRING	Null	Avaya J169/J179 IP Phone supports SNMPv3
SSH_ALLOWED	0	Disables SSH.
NVVPNMODE	0	VPN not supported in the FIPS mode.
VPNPROC	0	VPN not supported in the FIPS mode.
TPSLIST	Null	Push server does not support TLS.
VLANSEP	1	Enables VLAN separation that restricts the computer connected to the PC port from connecting to the phone VLAN.
VLANSEPMODE	1	Enforces VLAN separation. When set to 1, VLAN separation is enforced for both untagged and tagged packets from the computer and the network port. The computer cannot send tagged or untagged packets to the deskphone processor.
L2QVLAN	Address of the voice VLAN	The deskphone sends the untagged data packets to this VLAN. The value must not be 0 or the PHY2VLAN address.
L2Q	0: Auto 1: On	0: Auto - The deskphone starts sending tagged packets to the voice VLAN. If the VLANTEST timer has expired, the phone sends untagged packets. 1: Tagging – The deskphone starts sending tagged packets on voice VLAN and if VLANTEST timer expires, the phone then sends tagged packets on VLAN==0.
PHY2VLAN	Address of the data VLAN	The deskphone sends the tagged data packets to this VLAN. The value must not be 0 or the L2QVLAN address.

Table continues...

Parameter	Value	Description
CERT_WARNING_DAYS	60	Applies to trusted certificates, OCSP certificates, and identity certificate. Specifies the number of days before the expiration of a certificate that a warning should first appear on the phone screen. Log and syslog messages are generated for expired certificates. Valid values are 0 to 99. The value 0 disables the warning.
Console port	Disabled	Restricts the access to the console port. The serial port under <code>CRAFT > DEBUG</code> must be set to Adjunct.
WMLIDLEURI	Null	Disables the WML browser on the deskphone.
WMLHOME	Null	Disables the WML browser on the deskphone.
AUTOANSSTAT	0	Disables auto-answer.
GUESTLOGINSTAT	0	Disables the guest login feature.
VUMCIPADD	Null	Disables the visiting user login.

Related links

[JITC security compliance mode overview](#) on page 79

[JITC security compliance mode overview](#) on page 79

Error conditions

Assuming proper administration, most of the problems reported by phone users are likely to be LAN-based or Quality of Service. Server administration and other issues can impact user perception of IP phone performance.

Related links

[Administrative requirements](#) on page 73

Chapter 6: Maintaining an Avaya IP Phone

Upgrading the device

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

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

Related links

[Downloading and saving the software](#) on page 222

[Upgrading the device manually](#) on page 223

[Downloading text language files](#) on page 224

[Avaya J100 Expansion Module upgrade](#) on page 224

Downloading and saving the software

Before you begin

Ensure that your file server is set up.

Procedure

1. Go to the [Avaya Support](#) website.
2. In the **Enter Your Product Here** field, enter Avaya J100 Series IP Phones .
3. In the **Choose Release** field, click the required release number.
4. Click the **Downloads** tab.
The system displays a list of the latest downloads.
5. Click the appropriate software version.
The system displays the Downloads page.
6. In the **File** field, click the zipped file and save the file on the file server.
7. Extract the zipped file and save it at an appropriate location on the file server.

8. From the latest downloads list, click the settings file.

The system displays the Downloads page.

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

Related links

[Upgrading the device](#) on page 222

Upgrading the device manually

About this task

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

IP Office auto generates `96x1Hupgrade.txt` and `46xxsettings.txt` files. These files must be used in IP Office environment.

Procedure

1. Stop the file server.
2. Specify the port settings for HTTP or TLS in the HTTPPORT or TLSPOST settings respectively.
3. Perform a back up of all the current file server directories.
4. Copy the `46xxsettings.txt` file to a backup location.
5. Remove all the files in the download directory. This ensures that you do not have an inappropriate binary or configuration file on the server. The only system values that can be used in the conditional statement are: BOOTNAME, GROUP, MACADDR, MODEL, and SIG.
6. Remove all the files in the download directory. This ensures that you do not have an inappropriate binary or configuration file on the server.
7. Download the self-extracting executable file or the corresponding zip file.
8. Extract all the files.
9. Copy the `46xxsettings.txt` file to the download directory.
10. Modify the `46xxsettings.txt` file as required.
11. Restart the HTTP/HTTPS server.
12. Reset the phone.

Related links

[Upgrading the device](#) on page 222

Downloading text language files

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

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

 **Note:**

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

Related links

[Upgrading the device](#) on page 222

Avaya J100 Expansion Module upgrade

You can upgrade the Avaya J100 Expansion Module firmware to a new version using the software distribution package on the [Avaya Support](#) website. For more details, see [Upgrading the expansion module](#) on page 225.

During the boot-up, the phone will download the new firmware for the Avaya J100 Expansion Module.

After the phone downloads the expansion module firmware, the upgrade process will continue in the background.

 **Note:**

Reboot the phone if Avaya J100 Expansion Module connection is lost after the upgrade process is completed.

The upgrade procedure for an Avaya J100 Expansion Module takes up to 1 hour 30 minutes for each attached module. During this time, the expansion module is operable, you can make and receive calls with it and have access to other functionality.

When the upgrade is complete, the Avaya J100 Expansion Module displays the following notification: "Updated firmware has been downloaded. This device will be out of service for 3 minutes to apply the update. It will be applied automatically between 12am and 3am". Press the corresponding line button for **Apply now** or **Apply tonight** option to select the suitable upgrade time.

*** Note:**

When the Upgrade notification is displayed, the expansion module backlight is not turned off.

Related links

[Upgrading the device](#) on page 222

[Upgrading the expansion module](#) on page 225

Upgrading the expansion module**About this task**

Use this task to upgrade Avaya J100 Expansion Module firmware to a new version.

Before you begin

Download Avaya J100 Series IP Phones software distribution package from the <https://support.avaya.com/> website. See [Downloading and saving the software](#) on page 222 for more details.

Procedure

1. Extract the zipped file with the expansion module firmware and save it at an appropriate location on the file server.
2. Set the expansion module firmware file name in `96x1Hupgrade.txt`.
3. Reboot the phone. The expansion module will reboot automatically.

Related links

[Avaya J100 Expansion Module upgrade](#) on page 224

Software distribution packages

Software packages for the phones are available at the Avaya support site. These files are packaged together in a Zip format. Download the appropriate package from the [Avaya support site](#).

*** Note:**

The H.323 Sonic deskphones with hardware version 3 and above use `*.bin` while the phone with hardware version lesser than 3 use `*.tar`.

Avaya J100 Series IP Phones uses only `*.bin`.

The software distribution packages contain the following:

- Software files.
- One upgrade file such as `96x1Hupgrade.txt`.
- All the display text language files. For example, `mlf_SB189_v78_korean.txt`

- A file named `av_prca_pem_2033.txt` that contains a copy of the Avaya Product Root Certificate Authority certificate in PEM format. You can download this file to the phones based on the value of the TRUSTCERTS parameter.
- Updated MIB file.
- A file named `release.xml` that is used by the Avaya Software Update Manager application.

The Zip distribution packages includes a signatures directory. The signatures directory contains SHA-1 and SHA-2 signature files, and a certificate file for the Utility server.

 **Note:**

When you download the application file from the Avaya support Web site, ensure you are downloading the correct version. One version enables VPN and media encryption functionality, while the other disables those functions.

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

Two configuration files are:

- The upgrade file, that notifies the phone to upgrade software. The phone attempts to read this file after a reset. The upgrade file also contains directions to the settings file.
- The settings file contains the option settings that enable, disable, or otherwise customize the settings you might need to tailor the Avaya IP phones for your enterprise.

You can use one settings file for all your Avaya IP deskphones.

The H.323 IP Sonic deskphones with hardware version greater than 3 support only R6.6.2 and above.

Upgrading software packages

You can use the upgrade file and the application files included in the Software Distribution Package that Avaya provides to upgrade the phones. Do not modify the upgrade files. You must save all the essential files on your file server. When you download a new release onto a file server that has an existing release:

1. Stop the file server.
2. Administer the required port setting in HTTPPORT or TLSPOINT for HTTP or TLS, respectively if you want to specify a port the phones must use to communicate with the file server.

 **Note:**

IP phone H.323 v6.6.2 and later do not support HTTPS with MV_IPTTEL or IIS 6. It is recommended to upgrade to the current version of an HTTPS server that supports TLS 1.2.

3. Back up all the current file server directories as applicable.
4. Copy the `46xxsettings.txt` file to a backup location.
5. Remove all the files in the download directory. This ensures that you do not have an inappropriate binary or configuration file on the server. The only system values that can be used in the Conditional statement are: GROUP, MACADDR, MODEL, MODEL4, VPNACTIVE, and SIG_IN_USE.

Download the self-extracting executable file or the corresponding zip file.

6. Extract all the files.
7. Copy the `46xxsettings.txt` file back into the download directory.
8. Modify the `46xxsettings.txt` file as required.
9. Restart the HTTP and the HTTPS server.

You can download the default upgrade file from <http://www.avaya.com/support>. With this file, the phone uses default settings for customer-definable options.

These settings can also be changed with DHCP or in some cases, from the dial pad of the phone.

You might want to open the default file and administer the options to add useful functionality to your Avaya IP phones. Ensure that the file resides in the same directory as the upgrade file and named as the file as the `46xxsettings.scr` or `46xxsetting.txt`. The Avaya IP phones can operate without this file.

 **Note:**

Most Windows systems interpret the file extension `*.scr` as a screen saver. The 4600 IP phones originally used `*.scr` to indicate a script file. The settings file must have the extension `*.txt`.

Contents of the settings file

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

- Tags that are lines that begin with a single pound (#) character followed by a single space character and a text string with no spaces.
- **Goto** commands, of the form `GOTO tag`. **Goto** commands cause the phone to continue interpreting the settings file at the next line after a `#tag` statement. If such a statement does not exist, 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. You can use the following parameters in a conditional statement: GROUP, MACADDR, MODEL, MODEL4, VPNACTIVE and SIG_IN_USE.

- **SET** commands, of the form `SET parameter_name value`. The system ignores any invalid values for the associated *parameter_name* so the default or previously administered value is retained. All values must be text strings, even if the value itself is numeric or a dotted decimal IP Address.
- Comments, which are statements with a pound (#) character in the first column.

*** Note:**

Enclose all data in quotation marks for proper interpretation.

- **GET** commands, of the form `GET filename`. If the phone downloads the file named as filename, the phone interprets the file as an additional settings file and does not interpret additional lines in the original file. If the phone cannot obtain the file, the telephone continues to interpret the original file.

The Avaya-provided upgrade file includes lines that direct the phone to `GET 46xxsettings.txt` and `46xxsettings.scr`.

These lines cause the phone to use HTTP/HTTPS to attempt to download the file specified in the **GET** command. If the phone obtains the file, its contents are interpreted as an additional script file. If the file cannot be obtained, the phone continues processing the upgrade script file.

The phone processes the upgrade script file so that if there is no `46xxsettings.scr` file, the phone looks for the `46xxsettings.txt` file. If the phone obtains the settings file successfully but does not include any setting changes the phone stops using HTTP. This process happens when you initially download the script file template from the Avaya Support website, before you make any changes. When the settings file contains no setting changes, the phone does not go back to the upgrade script file.

You can customize the settings file and identify non-default option settings, application-specific parameters, and other settings. You can download a template for this file from the [Avaya Support website](#).

Specify settings that are different from default values, although you can also specify default values.

Related links

[Settings file parameters retained during reboot](#) on page 228

Settings file parameters retained during reboot

During a reboot, if the deskphone is unable to access the `46xxsettings.txt` file, it does not retain the values of all the parameters. To identify whether the parameter is retained or not retained, refer to the table below.

Parameter	Retained
AGCHAND	Y

Table continues...

Parameter	Retained
AGCHEAD	Y
AGCSPKR	Y
AGTCALLINFOSTAT	Y
AGTFWDBTNSTAT	Y
AGTGREETINGSTAT	Y
AGTLOGINFAC	Y
AGTLOGOUTFAC	N
AGTSPKRSTAT	Y
AGTTIMESTAT	N
AGTTRANSLPRI	Y
AGTTRANSLPK	Y
AGTTRANSLCLBK	N
AGTTRANSLTO	Y
AGTTRANSLICOM	Y
AGTVUSTATID	Y
AGTACTIVESK	N
APPNAME	N
APPSTAT	Y
AUDIOENV	Y
AUDIOSTHD	Y
AUDIOSTHS	Y
AUTH	Y
BAKLIGHTOFF	Y
BRAUTH	Y
BRURI	Y
CALCSTAT	Y
CALLCTRSTAT	Y
CLDELCALLBK	Y
DHCPSTD	Y
FBONCASCREEEN	Y
GUESTDURATION	N
GUESTLOGINSTAT	N
GUESTWARNING	N
HEADSYS	N
HOMEIDLETIME	N

Table continues...

Parameter	Retained
LOGBACKUP	Y
LOGMISSEDONCE	Y
LOGSRVR	N
LOGLOCAL	Y
LOGUNSEEN	Y
LANGSYS	N
LANGxFILE	Y
LANG0STAT	N
MSGNUM	N
OPSTAT	Y
OPSTAT2	Y
OPSTATCC	Y
PROCSTAT	Y
PROCPSWD	Y
PHY1STAT	Y
PHY2STAT	Y
PHNCC	Y
PHNDPLENGTH	Y
PHNIC	Y
PHNLDLENGTH	N
PHNLD	Y
PHNOL	Y
PHNSCRALL	N
QKLOGINSTAT	Y
RFSNAME	N
REREGISTER	N
SNMPADD	Y
SNMPSTRING	Y
SIG	Y
SCREENSAVERON	Y
SCREENSAVER	Y
TIMERSTAT	N
TPSLIST	N
UNNAMEDSTAT	Y
VLANTEST	Y

Table continues...

Parameter	Retained
VPNPROC	Y
WORLDLOCKAPP	N
WEATHERAPP	N
WMLHOME	N
WMLPORT	N
WMLPROXY	N

Related links

[Contents of the settings file](#) on page 227

Downloading text language files

About this task

You must save the language files used for text entry and display purposes in the same location as the `46xxsettings.txt` file or in the HTTP Server directory. The HTTP Server directory is defined using the `SET HTTPDIR HTTP server directory path` command.

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 LANGxFILE` command in the `46xxsettings.txt` file before downloading a language file with the same filename.

Changing the signaling protocol

About this task

For enterprises requiring both H.323 and SIP-based protocols, you can specify the protocol for all or specific deskphones in the following two ways:

Procedure

1. As of Release 6.0, you can set the SIG parameter in DHCP Option 242 (Site-Specific Option Number) or in the `46xxsettings.txt` file.

This setting will apply to all telephones except those for which SIG has been manually configured to a value of H.323 or SIP using the SIG Craft procedure.

2. You can set the SIG parameter on a per-phone basis using the SIG Craft procedure.

Applying settings to logical groups

You might have different communities of end users with the same phone model but requiring different administered settings. For example, you might want to restrict Call Center agents from logging out, an essential capability for *hot-desking* associates. This section provides examples of the group settings for each of these situations.

You can separate groups of users is to associate each of them with a number. Use the GROUP parameter for this purpose. You cannot set GROUP system value in the `46xxsettings.txt` file. The GROUP parameter can only be set on a phone-by-phone basis. To set the GROUP parameter, first identify which phones 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. The largest group is assigned as Group 0.

Then, at each phone that does not have default parameters, instruct the installer or end-user to invoke the GROUP Local Administrative Craft procedure. After the GROUP assignments are in place, edit the configuration file to allow each phone 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 CALLCENTER IF $GROUP SEQ 2 goto HOTDESK {specify
settings unique to Group 0} goto END

# CALLCENTER {specify settings unique to Group 1} goto END

# HOTDESK {specify settings unique to Group 2}

# END {specify settings common to all Groups}
```

Calibrating the touch screen

About this task

Use screen calibration for alignment of the touch screen of 9621G and 9641G deskphones. Use a stylus instead of your finger to touch the calibration points precisely. The CLEAR Craft procedure clears any calibration data set using the Craft Procedures screen, but does not change factory settings of calibration data. Use the **Default** softkey to restore factory-set calibration. You cannot save calibration results as part of a backup operation. 9641GS deskphones do not support screen calibration.

Procedure

1. Select **CALIBRATION** from the Craft Procedures screen.

The telephone displays three softkeys **Start**, **Default**, and **Cancel**.

2. Touch **Start** to calibrate the screen.

The screen displays a calibration target with a plus sign (+) at a particular point.

3. Touch the center of the target with the stylus as soon as the target appears.

The target disappears, and a new target appears in a different part of the screen.

4. Touch the center of each target with the stylus within 10 seconds of its appearance.

After you touch all the five targets, the system plays a confirmation tone sound and displays `Calibration successful. Press Save to store the new calibration data message.`

5. Touch **Save** to return to the Craft Procedures screen.

The system stores the calibration results in the nonvolatile memory of the telephone.

Adjusting contrast on the button module

About this task

Use the following procedure to adjust the contrast of the button module attached to the phone. Fifteen contrast levels are available.

Note:

The contrast setting is not supported on the Avaya J100 Expansion Module.

Procedure

1. Select **CONT** from the **Main Menu > Option & Settings > Screen & Sound Options > Contrast...**

The phone prompts you to use the Right and Left navigation arrows to change the contrast for button module shown as Module: 1 or the contrast for the phone shown as Phone: contrast.

2. To change the setting, press the **Right** or **Left** navigation arrow to navigate through the settings.

By default, the contrast button is set to the middle of the contrast setting. As you press the navigation arrow, the next higher or lower contrast level is selected and displayed as the setting.

3. If more than one button module is attached, scroll down to that line, for example, to Module: 2 and repeat Step 2 to change the contrast.
4. Press **Save** to store the new contrast settings and display the Craft Procedures screen.

Adjusting contrast on button modules and non-color deskphones

About this task

Use the following procedure to adjust the contrast of any button module when attached to any phone or any non-color IP deskphone. Fifteen contrast levels are available.

Procedure

1. Select **CONT** from the **Main Menu > Option & Settings > Screen & Sound Options > Contrast...**

The deskphone prompts you to use the Right and Left navigation arrows to change the contrast for button module shown as Module: 1 or the contrast for the deskphone shown as Phone: contrast.

2. To change the setting, press the **Right** or **Left** navigation arrow to navigate through the settings.

By default, the contrast button is set to the middle of the contrast setting. As you press the navigation arrow, the next higher or lower contrast level is selected and displayed as the setting.

3. If more than one button module is attached, scroll down to that line, for example, to Module: 2 and repeat Step 2 to change the contrast.
4. Press **Save** to store the new contrast settings and display the Craft Procedures screen.

Disabling or enabling automatic gain control

About this task

Use the following procedure to turn Automatic Gain Control (AGC) for the handset, headset, or to put the speaker to On or Off. The user can potentially override the AGC local procedure settings. If the values are changed, the backup file stores the AGC values set by the user and does not save any setting established using this local procedure.

Procedure

1. Select **AGC** from the Craft Procedures screen.

The phone displays the options as shown in the following table:

Options available for AGC	Status
Handset Auto Gain control	On
Headset Auto Gain Control	On
Speaker Auto Gain Control	On

The text string associated with the current system value of NVAGCHAND, NVAGCHEAD, or NVAGCSPKR are defined as:

- **On** if the respective NVAGCXXXX system value is 1.
 - **On** if the respective NVAGCXXXX system value is 0.
2. Select the appropriate line and press **Change** to toggle it to On or Off as required.
 3. Press **Save** to store the new setting, update the associated system value, and display the Craft Procedures screen.

Setting handset audio equalization

Procedure

1. Select **CONT** from the **Main Menu > Option & Settings > Advanced Options > Handset Equalization...**

The Handset Equalization Procedure screen displays the currently used audio equalization under **Current Setting** and lists the following options under **New Setting** for selection.

- **Default:** USER_HSEQUAL set value 0
 - **Audio-Opt :** USER_HSEQUAL set value 1
 - **HAC Opt :** USER_HSEQUAL set value 2
 - **Amplified :**USER_HSEQUAL set value 3
2. Use the navigation arrows to select an audio equalization.

The audio equalization options are a combination of internal parameters consisting of the audio equalization specifications of the settings file, user option, and Local Procedure. These are:

- **Default:** TIA-810/920 and S004
- **Audio Opt:** TIA-810/920 and S004
- **HAC Opt:** HAC

The only difference between **Default** and **Audio Opt** is that for **Audio Opt**, either the settings file, the user option, or the Local Procedure has explicitly selected TIA-810/920 and S004.

3. Press **Save** to store the new setting and display the Craft Procedures screen.

Changing the group identifier

About this task

When updating the local Craft procedure or Admin menu procedures press the appropriate softkey on IP phone.

Note:

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

Procedure

1. Select **GROUP** from the Craft Procedures screen.

The following text is displayed:

- **Current Setting**
- **New Setting**

where **Current Setting** is the current system value of NVGROUP.

2. In the **Group** text box, enter a valid **Group** value from 0 to 999.
3. Press **Save** to store the new setting. The deskphone displays the Craft Procedures screen.

The deskphone displays the Craft Procedures screen.

Chapter 7: Data Privacy for 9600 and J100 IP Phones H.323

Data Privacy detailed description

Data Privacy Controls

This addendum applies to Avaya 9600 Series and Avaya J100 Series IP Phones version 6.8.3.0 and later.

General

The following sections describe what user information is being handled by 9600 and Avaya J100 Series IP Phones, whether this information stored locally on the phone or sent over the network, how it is being stored and ways to manage this information.

User information

At first, the following user information is being handled:

- User call logs
- User contacts
- User H.323 registration password
- IPSec VPN User password
- Device IP address
- Backup/restore HTTP credentials
- User display name
- Guest login H.323 registration password
- Button module labels

User information storage or sending over the network

User call logs are stored locally on the device in non persistent storage for example RAM, after any reboot or turn on power the call logs are erased from the device and only fetched from HTTP/HTTPS file server if BRURI is defined and a backup file for the specific extension exists. Calls to the extension while the extension is logout are stored on Avaya Aura[®] Communication Manager

and retrieved by the phone when doing login. Call logs can be stored on external file server and can be sent/received using HTTP or HTTPS.

User contacts are stored locally on the device. Contacts can be stored on external file server and can be sent/received using HTTP or HTTPS.

H.323 registration password is stored locally on the device and used for manual login for first time login and auto login whenever the phone is reboot or powerup. In the same way, Guest user H.323 registration password is stored locally on the device. The regular and guest users H.323 password derivatives are sent over the network as part of the H.323 registration process.

VPN user password is stored locally on the device and used for IPSec VPN connection.

Device IP address is stored locally and reported also to the H.323 gatekeeper for information about the specific extension. Administrator can view the IP address using "status station" SAT screen on the Avaya Aura® Communication Manager. Device IP address might be collected by any service which the phone open connection to it for logging purposes. Such as VPN gateway, File server, etc.

Backup/restore credentials are stored locally on the device and sent over the network using basic, digest or NTLM authentication.

User display name is configured in the H.323 gatekeeper (for example, in CM station SAT screen) and presented in other endpoints when there is an active call.

Button labels are user assigned labels for different calls features including auto dials. Button labels are stored locally on the device. Button labels can be stored on external file server and can be sent/received using HTTP or HTTPS.

Encryption of user information

Please note that all user information specified above is not saved encrypted on the phone storage. The passwords are encrypted on flash from release 6.8.3. The calls logs and contacts are also stored in clear on the file server. The backup filename includes the extension number or agent number and the phone shall retrieve only the relevant login extension or agent information.

Access to user data

The phone supports SSH server which is protected using Avaya Enhanced Access Security Gateway (EASG) authentication. The SSH server by default is disabled but using CRAFT menus access it can be enabled using administrator password. The administrator password is configured using 46xxsettings.txt file or H.323 gatekeeper. The administrator password is numeric only. SSH_ALLOWED can be used to permanently disable SSH server on the phone. Avaya authentication file can be used to enable console port or SSH server in root file. Only Avaya technicians can install such file using SSH craft access. The file is limited by time and can be disabled using AUTHCTRLSTAT. User information can be viewed locally using SSH server or console port.

The call history and contacts are also presented on the phone screen. Station Lock mechanism can be used to prevent such access when user is not in office. Users shall actively lock their phones when they leave the office. Another option is to do logout when leaving the office and do

login when entering the office. Missed calls when the extension is not logout are collected by the H.323 gatekeeper (e.g. Avaya communication manager). The backup file on the file server includes user call logs and contacts. The backup file is stored clear on the file server. Administrator shall protect this server to have access to endpoints with certain credentials and identity certificate.

Data retention

Data retention of user information is not limited by time. However, there is enforced limit on the numbers of call logs stored (100) and above this limit new call logs will override old calls logs.

Management of user data

User data can be deleted in one of the following ways:

Administrator

- CLEAR – return to factory defaults operation which clear all user and administrator data including local log files. There is no specific operation for administrator to delete phone local log files.
- While the extension is logout, administrator can login into the file server and deletes the specific backup file of the specific extension.
- APPSTAT configured in the 46xxsettings.txt file can be used to disable call logs and contacts management by end users.

User

- Any new user login erases all previous user data. I.e. login to the phone with other extension, deletes previous user data.
- User can delete ALL their calls logs using single operation in the phone's history application.
- User can delete their contacts – each contact shall be deleted manually.
- User can return personal button labels to factory using single operation available in the phone settings.

Additional operations by end users

- User can reboot or turn on power of the phone to delete call logs as they are stored in non-persistent memory for example RAM. Please note that if BRURI is defined call logs are retrieved from the HTTP/HTTPS file server.
- Users can manage all their own information. User preferences are configured in the phone settings menus.
- User can disable call log application (by default, enabled).

Please note that administrator can change user information stored on the file server while the phone is NOT logged-in by accessing the file server. The backup file is stored in clear and without digital signature which allows administrator modification.

Recommendation for better securing user information

Backup/Restore calls logs, contacts and button labels (regular user and guest user login)

If the user is working with his/her own phone only and do not login to his/her extension on other phones, then it is recommended to disable the backup/restore file server (set BRURI ""). If this is not the case, then it is recommended to use HTTPS file server for backup/restore of calls logs, contacts and button labels. In addition, there shall be a unique backup/restore credentials for each user and the HTTPS file server shall support mutual certificate authentication to restrict accessing the user information stored on the file server from any other devices beside Avaya hard endpoints. The Backup/restore file server shall be well protected from other users access to prevent access to the backup/restore files.

Sending H.323 password over the network (regular user and guest user login)

There are 3 registration options defined in the ip-network-region SAT screen when using Avaya Aura® Communication Manager (same options are supported by IP Office Manager): "challenge" (Password MD5 digest), pin-ike (Annex-H) and "H323TLS". It is recommended to use "H323TLS" to secure both signaling and SRTP key information. H323SIGPROTOCOL can be set to "2" to enforce use of H323 signaling over TLS by the phone itself (and not rely on the H.323 gatekeeper policy).

SRTP for media encryption

SRTP shall be enabled to ensure audio media streams are encrypted (using AES-128 only). SRTCP is not supported and RTCP is disabled if not needed for QoS monitoring. RTCP provides information about the extension used. SRTP or RTCP configuration is provided by the H.323 gatekeeper (for example, IP-network-region SAT screen in CM).

TLS1.2 configuration

9600 and Avaya J100 Series IP Phones H.323 supports TLS 1.2 for all services. It is recommended to set TLS_VERSION to 1 to enforce TLS 1.2 usage (and avoid TLS 1.0). This configuration means that the phone will connect to a server which supports TLS1.2. All phone's service MUST support at least TLS 1.2 (this includes H.323 gatekeeper, HTTPS file server, etc).

Enable H.323 station lock

Add feature button sta-lock in the station SAT screen on Avaya communication to provide station lock feature. When enabled, there is no option to access call-logs, contacts and settings menus. To disable, user is required to enter the H.323 registration password. Recommend users to lock their device when not in their place. H.323 gatekeeper such as Avaya Aura® Communication Manager provides automatic station lock per time of days rules using CM SAT screen tod-station-lock. The Time of Day Station Lock Table can be associated specifically for each station. This can be used to enhance the privacy of the end users.

SSH server and authentication file configuration

To avoid SSH access to the device, please make sure that SSH_ALLOWED is permanently disabled (0). In addition, to avoid opening console port please make sure that AUTHCTRLSTAT is set 0.

Administrator password

The administrator password shall be configured in the H.323 gatekeeper only (example Avaya Aura® Communication Manager) and shall not be configured using the 46xxsettings.txt file. The password shall be with maximum length of digits (7).

Logging

It is recommended to disable remote logging using Syslog as syslog events are stored in clear over UDP (by default, disabled). LOGSRVR shall be set to "" (default). In addition, SNMP shall be disabled (default value) as the SNMP tables can be accessed using SNMPv1 only (clear, unauthenticated access). The endpoints provide logging information using MIB tables. SNMPSTRING shall be set to "" (default value). Please note that debug logs may include user information. The debug logs are stored in clear. The debug logs are limited in space and old log entries are deleted by new logs entries when log file size limit is reached. CLEAR (return to factory defaults) operation available in administrator menus, erases the debug logs. The debug logs are accessible through SSH/Console if SSH server/Console port is enabled by Avaya services only. To reduce information collected internally for debug logging purposes, LOGTOFILE (default, disabled) configured in the settings file or in the administrator DEBUG menu shall be disabled. In addition, LOGLOCAL shall be set to "0" (disabled).

Data privacy controls for Avaya J100 Series H.323 and 9600 IP Phones

This addendum applies to Avaya J100 Series IP Phones H.323 IP Phones and 9600 Series IP Deskphones.

Personal Data is stored internally in the phone's flash filesystem which is not directly externally accessible except through SSH to the limited privilege "craft" user through an Avaya EASG login. Filesystem content is not encrypted, passwords are now encrypted in release 6.8.3, and contacts and call logs (contacts are stored on flash). However, passwords stored on flash are encrypted. Call logs are not stored on persistent storage (for example flash), but rather on non-persistent storage (for example RAM). When Personal Data is being transmitted over a network, it is encrypted with the most up-to-date protocols.

Related links

[Data Categories Containing Personal Data \(PD\)](#) on page 242

[PD Human Access Controls](#) on page 242

[PD Programmatic or API Access Controls](#) on page 243

[PD at Rest Encryption Controls](#) on page 243

[PD in Transit Encryption Controls](#) on page 244

[PD Retention Period Controls](#) on page 244

[PD Export Controls and Procedures](#) on page 245

[PD View, Modify, Delete Controls and Procedures](#) on page 245

[PD Pseudonymization Operations Statement](#) on page 246

Data Categories Containing Personal Data (PD)

User data (in memory)

Calls: Remote party phone number

Conference calls: participant display name, roster list

End user preferences information H.323 extension password, VPN user password

Contacts retrieved from network

User data (on flash)

End user preferences information H.323 extension password, VPN user password

Contacts retrieves from network

Backup/restore user credentials

Call Logs (in memory)

Local call logs

User Passwords (on flash)

H323 extension credentials, backup/restore HTTP password

User data in logs (on flash)

- Backup or restore credentials are stored in RAM. The passwords stored in flash.
- User handle, user name, display name information from H323 messages. Syslogs are not encrypted.

Related links

[Data privacy controls for Avaya J100 Series H.323 and 9600 IP Phones](#) on page 241

PD Human Access Controls

User data (in memory)

- No Access

User data (on flash)

- SSH – Limited to Avaya Services login to “craft” account with EASG authentication. “craft” account has limited access to filesystem. Console port can be opened from the administrator menu once enabled by Avaya services using SSH with EASG and a special authentication file that loaded into the phone (96x1/J159/J169/J179/J189/B189 H.323).

Call Logs (in memory)

- Calls logs are stored in RAM.

User Passwords (on flash)

- No Access

User data in logs (on flash)

- SSH – Limited to Avaya Services login to “craft” account with EASG authentication. “craft” account has limited access to filesystem. Console port can be opened from the administrator

menu once enabled by Avaya services using SSH with EASG and a special authentication file that loaded into the phone (96x1/J159/J169/J179/J189 H.323).

Related links

[Data privacy controls for Avaya J100 Series H.323 and 9600 IP Phones](#) on page 241

PD Programmatic or API Access Controls**User data (in memory)**

- Internal programmatic access.

User data (on flash)

- None

Call Logs (in memory)

- None

User Passwords (on flash)

- None

User data in logs (on flash)

- None

Related links

[Data privacy controls for Avaya J100 Series H.323 and 9600 IP Phones](#) on page 241

PD at Rest Encryption Controls**User data (in memory)**

- Not encrypted by phone application.

User data (on flash)

- Not Encrypted

Call Logs (in memory)

- Not Encrypted

User Passwords (on flash)

- There are no controls available for the type or strength of encryption.
- Passwords are encrypted on flash from release 6.8.3, other user information stored in flash is not encrypted.

User data in logs (on flash)

- Not Encrypted

Related links

[Data privacy controls for Avaya J100 Series H.323 and 9600 IP Phones](#) on page 241

PD in Transit Encryption Controls

User data (in memory)

- TLS 1.2 to send/receive data with servers

User data (on flash)

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

Call Logs (in memory)

- TLS 1.2 (HTTPS/H.323 signaling over TLS) to receive data with servers

User Passwords (on flash)

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

User data in logs (on flash)

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

Related links

[Data privacy controls for Avaya J100 Series H.323 and 9600 IP Phones](#) on page 241

PD Retention Period Controls

User data (in memory)

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

User data (on flash)

- Permanent until rolled over, or until the device is reset to defaults or new user login.

Call Logs (in memory)

- Call logs can be erased during reboot or power-up.
- Permanent until rolled over, manually deleted by the user, or until the device is reset to defaults or new user login.

User Passwords (on flash)

- Permanent until rolled over, or until the device is reset to defaults or a new user login.

User data in logs (on flash)

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

Related links

[Data privacy controls for Avaya J100 Series H.323 and 9600 IP Phones](#) on page 241

PD Export Controls and Procedures

User data (in memory)

- Not applicable.

User data (on flash)

- Using the phone Administration menu, an Administrator can generate a Phone Report containing configuration data which is transmitted if an external backup server is configured via the BRURI setting.
- While logged in to “craft” via SSH, configuration data can be transmitted

Call Logs (in memory)

- No export capability is provided

User Passwords (on flash)

- No export capability is provided

User data in logs (on flash)

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

Related links

[Data privacy controls for Avaya J100 Series H.323 and 9600 IP Phones](#) on page 241

PD View, Modify, Delete Controls and Procedures

User data (in memory)

- Not applicable

User data (on flash)

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

Call Logs (in memory)

- The User can delete individual log entries or all log entries from the local menu on the phone
- The Administrator can delete all call logs using the Reset to Defaults function in the Administration menu on the phone
- New user login deletes all previous user data
- Power up or Reset of the device can erase call logs.

User Passwords (on flash)

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

- New user login deletes all previous user data

User data in logs (on flash)

- The User has no ability to modify or delete log files
- The Administrator can delete all log files in the phone using the Reset to Defaults function in the Administration menu on the phone

Related links

[Data privacy controls for Avaya J100 Series H.323 and 9600 IP Phones](#) on page 241

PD Pseudonymization Operations Statement

User data (in memory)

- Not applicable

User data (on flash)

- Not applicable

Call Logs (in memory)

- Not applicable

User Passwords (on flash)

- Not applicable

User data in logs (on flash)

- Not applicable

Related links

[Data privacy controls for Avaya J100 Series H.323 and 9600 IP Phones](#) on page 241

Chapter 8: Troubleshooting

Resolving error conditions

About this task

Installers can troubleshoot problems before seeking assistance from the system or LAN administrator in four areas:

Procedure

1. Check both the power and Ethernet wiring for the following conditions:
 - Check whether all components are plugged in correctly.
 - Check LAN connectivity in both directions to all servers - DHCP, HTTP, HTTPS, DEFINITY®/MultiVantage™.
 - If the deskphone is powered from the LAN, ensure that the LAN is properly administered and is compliant with IEEE 802.3af.
2. If you use static addressing:
 - Use the VIEW option to find the names of the files being used and verify that these filenames match those on the HTTP/HTTPS server. Check the Avaya Support site at www.support.avaya.com to verify whether the correct files are being used.
 - Use the ADDR option to verify IP addresses.
3. If the deskphone is not communicating with the system, DHCP, HTTP, or Avaya Media Server, make a note of the last message displayed.

Consult the system administrator. Sometimes, you can correct problems relating to Communication Manager and HTTP communications by setting the HTTPPORT value to 81 which is the port required for HTTP downloads rather than the using the default.
4. If you want the deskphone to be IEEE-powered, verify with the LAN administrator that IEEE power is indeed supported on the LAN.

Failure to hear DTMF tones

As H.323 telephones do not send DTMF tones to non-H.323 telephones, the user need not perform troubleshooting for failure to hear DTMF tones from a IP phone. The TN2302AP board does not pass in-band DTMF tones.

Correcting a power interruption

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

Using the VIEW procedure for troubleshooting

About this task

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

 **Note:**

If administered through OPSTAT, end users can gain access to the Network Information option from the *Phone Settings* option of Avaya Menu to view but not change most of the parameters associated with Craft Local Procedures. For more information about this option, see the applicable user guides.

 **Important:**

IPv6 operation is limited to a specific customer set and is not available for general use.

 **Note:**

You can use the ADDR option to view IP addresses if needed. The IP addresses might have been entered incorrectly. Verify whether you were provided with correct IP addresses.

Procedure

1. Select **VIEW** from the Craft Local Procedure Screen.

The phone displays the following options: **IP Parameters**, **Quality of Service**, and **Miscellaneous** and **Interfaces**.

2. Tap the category that you want to see.

The information for that category is displayed.

 **Note:**

Use the Right navigation arrow to scroll through the viewable information.

Table 21: Parameter Values

Name	System Value	Format
Phone (IPv4)	<i>nnn.nnn.nnn.nnn</i>	Phone IP address, IPADD value.
Phone (IPv6)	<i>hhhh:hhhh::hhhh:hhhh:hhhh</i>	Phone IP address, NVIPADDV6 value.
Phone (IPv6LL)	<i>hhhh:hhhh::hhhh:hhhh:hhhh</i>	Phone IP address, IPADDV6LL value.

Table continues...

Name	System Value	Format
Call Server	<i>nnn.nnn.nnn.nnn</i>	IP address of the call server currently in use, otherwise <i>0.0.0.0</i> .
Supplicant	<i>cccccccccccccccc</i>	Text equivalent of DOT1XSTAT. If 0, Disabled; if 1, Unicast-only; if 2, Unicast/multicast.
Pass-thru	<i>cccccccccccccccc</i>	Text equivalent of DOT1X. If 0, Enabled; if 1, Enabled w/Logoff; if 2, Disabled.
Router (IPv4)	<i>nnn.nnn.nnn.nnn</i>	Up to 15 ASCII characters, the IP address of the router in use.
Mask (IPv4)	<i>nnn.nnn.nnn.nnn</i>	Up to 15 ASCII characters, NETMASK value.
HTTP server	<i>nnn.nnn.nnn.nnn</i>	IP address of last HTTP server used successfully during initialization or <i>0.0.0.0</i> . if no file server was used successfully.
HTTPS server	<i>nnn.nnn.nnn.nnn</i>	IP address of last HTTPS server used successfully during initialization or <i>0.0.0.0</i> . if no file server was used successfully.
802.1Q	<i>cccc</i>	Text string corresponding to the L2Q value.
VLAN ID	<i>cccc</i>	Up to 4 ASCII characters. Value is L2QVLAN text <i>Auto</i> if 802.1Q tagging is 0 or <i>On</i> if 802.1Q tagging is 1. If 802.1Q tagging is off (2), this line is not displayed.
VLAN Test	<i>ccc</i>	Up to 3 ASCII characters. Value is VLANTEST value if 802.1Q tagging is 0 or 1. If 802.1Q tagging is off (2), this line is not displayed.
Scroll Right to see the following additional parameters/values:		
L2 Audio	<i>n</i>	L2QAUD, layer 2 audio priority value.
L2 Signaling	<i>n</i>	L2QSIG, layer 2 signaling priority value.
L3 Audio	<i>nn</i>	DSCPAUD, Differentiated Services Code Point for audio.
L3 Signaling	<i>nn</i>	DSCPSIG, Differentiated Services Code Point for signaling.
Scroll Right to see the following additional parameters/values:		

Table continues...

Name	System Value	Format
Ethernet		Text string corresponding to PHY1STAT value, for example, <i>auto 100 Mbps HDX, 1000 Mbps FDX</i> .
PC Ethernet		Test string corresponding to PHY2STAT value, for example, <i>disabled, 100 Mbps HDX, 1000 Mbps FDX</i> .
Scroll Right to see the following additional parameters/values:		
Model	<i>96ccDccc</i>	Up to 8 ASCII characters, MODEL serial number.
Phone SN	<i>cccccccccccccccccc</i>	Phone Serial Number, up to 18 ASCII characters.
PWB SN	<i>cccccccccccccccccc</i>	Printed Circuit board Serial Number, up to 18 ASCII characters. Applies only to 96xx IP phones that have a software-readable PWB serial number and Comcode. * Note: This parameter is not supported in Release 6.3 and later.
PWB comcode	<i>nnnnnnnnnn</i>	Nine ASCII numeric characters. Applies only to 96xx IP phones that have a software-readable PWB serial number and Comcode. * Note: This parameter is not supported in Release 6.3 and later.
MAC address	<i>hh:hh:hh:hh:hh:hh</i>	Each octet of the MAC address displays as a pair of hexadecimal numbers.
Group	<i>nnn</i>	Up to three ASCII numeric characters: GROUP value.
Protocol:	<i>cccccccc</i>	Up to eight ASCII characters, currently only <i>H.323</i>
Application File	<i>filename.ext</i>	Four to 32 ASCII characters as primary application.
Ethernet	<i>cccccccc Ethernet</i>	Two to eight ASCII characters, either <i>1000 Mbps</i> , <i>100 Mbps</i> , <i>10 Mbps</i> , or <i>No</i> .

Table continues...

Name	System Value	Format
Kernel/RFS file	<i>bootcodename</i>	One to 32 ASCII characters (backup image name).
Backup App File	<i>filename.ext</i>	Four to 32 ASCII characters (backup application).
Button Module 1	<i>cccccccccccccc</i>	14 ASCII characters. Version identifier of the software in the first attached Button Module, if applicable.
Button Module 2	<i>cccccccccccccc</i>	14 ASCII characters. Version identifier of the software in the second attached button module, if applicable.
Button Module 3	<i>cccccccccccccc</i>	14 ASCII characters. Version identifier of the software in the third attached button module, if applicable.
Proxy Server	WMLPROXY	Proxy server used for WML functions.
Voice Language File	NVVOXFILE	Language file (NVVOXFILE) designated for voice-initiated dialing. Not applicable for software Release 6.0.

3. Use the Right navigation arrow to scroll through the information shown in the table.
4. Press **Back** at any time to return to the Craft Procedures screen.

Installation error and status messages

The phone displays messages in the currently selected language or in the language specified by the LANGSYS parameter value, if the phone is logged off. If English is not the selected language, the phone displays messages in English only when the message are associated with local procedures, for example, MUTE VIEW.

The phone displays most of the messages for only about 30 seconds, and then the phone is reset. The most common exception is *Extension in Use*, display more than 30 seconds and which remains until you perform any further action on the phone.

 **Note:**

For VPN-related error and status messages, see the *VPN Setup Guide for 9600 Series IP Telephones, 16-602968*.

Table 22: Possible error and status messages during installation of a phone

Message	Cause/Resolution
802.1X Failure	<p>CAUSE: Incorrect credentials provided for authentication or credentials not provided at all.</p> <p>RESOLUTION: Follow the display prompts and reenter the 802.1X ID and password.</p>
IPv4 or IPv6 address Conflict	<p>CAUSE: The phone has detected an IP address conflict.</p> <p>RESOLUTION: Verify administration settings to identify duplicate IP addresses.</p>
Authentication Error	<p>CAUSE: The call server does not recognize the extension entered.</p> <p>RESOLUTION: Confirm the extension is correct and is correctly administered on the switch. Then try registration again, and enter the extension accurately.</p>
Bad FileSv address	<p>CAUSE: The HTTP/HTTPS server IP address in the IP phone's memory is all zeroes.</p> <p>RESOLUTION: Depending on the specific requirements of your network, this may not be an error. If appropriate, either administer the DHCP server with the proper address of the HTTP/HTTPS server, or administer the phone locally using the ADDR option.</p>
Bad Router?	<p>CAUSE: The phone cannot find a router based on the information in the DHCP file for GIPADD.</p> <p>RESOLUTION: Use static addressing to specify a router address, or change administration on DHCP.</p>
Call Error	<p>CAUSE: The user was on a call when the connection to the gatekeeper went down due to a network outage or a gatekeeper problem. The phone attempted to automatically register with the same or another gatekeeper, but the responding gatekeeper had no record of the call.</p> <p>RESOLUTION: Wait for the call to end, and if the phone does not automatically register, restart the phone.</p>
Connecting...	<p>CAUSE: The phone is attempting to establish a TCP connection with the call server. A resource needed to establish the connection might not be available or the 10 second buffer on switch-related actions might have expired.</p> <p>RESOLUTION: Allow the phone to continue attempts to connect to TCP.</p>
Contacting call server...	<p>CAUSE: The phone has rebooted successfully and is attempting to register with the call server.</p> <p>RESOLUTION: Allow the phone to continue.</p>
DHCP: CONFLICT * to program	<p>CAUSE: At least one of the IP address offered by the DHCP server conflicts with another address.</p> <p>RESOLUTION: Review DHCP server administration to identify duplicate IP address(es).</p>

Table continues...

Message	Cause/Resolution
DHCPv6 Failure: (with message)	<p>CAUSE: The phone receives a reply message with a Status Code option that contains a status-code of 1 which means <i>UnspecFail</i> or a reply in response to a <i>Renew</i> or <i>Rebind</i> message with a Status Code option containing a status-code value other than 0 that indicates <i>Success</i> or 5 which indicates <i>UseMulticast</i>.</p> <p>RESOLUTION: In the first case, DHCPv6 will be restarted. If this message is the result of a status-code value other than 1 or 5, IPADDRV6 will be set to null; if dual-stack operation is enabled the phone will also cease use of its IPv4 address and IPADD will be set to null, and DHCP operation will proceed.</p>
Discover <i>aaa.bbb.ccc.ddd</i>	<p>CAUSE: The phone is attempting to find Communication Manager.</p> <p>RESOLUTION: Long display of this message implies failure of the Communication Manager server or a network problem that an administrator must fix. The administrator must ensure that there is network connectivity to Communication Manager, user extension is defined, and the Communication Manager server is up.</p>
Discovering...	<p>CAUSE: The phone is attempting to find a Communication Manager.</p> <p>RESOLUTION: Long display of this message implies failure of the Communication Manager server or a network problem that an administrator must fix. The administrator must ensure that there is network connectivity to Communication Manager, user extension is defined, and the Communication Manager server is up. The user can also press the RESET button for the phone to reboot, but this will erase the stored credentials.</p>
EEPROM error, repair required	<p>CAUSE: Application file was not downloaded or saved correctly.</p> <p>RESOLUTION: The phone automatically resets and attempts to re-initialize.</p>
Emergency Option	<p>CAUSE: Incompatible emergency option.</p> <p>RESOLUTION: This must not happen. Contact Avaya support.</p>
Extension in Use Extension in use: <NNNN> Press continue to take over this extension Login Continue	<p>CAUSE: The call server detects an extension conflict with an existing set or Softphone.</p> <p>RESOLUTION: By pressing Continue, you can force the current phone to register and thereby disconnect the other user. When Login is selected instead, the phone re-prompts for entry of a different extension and password.</p>
Finding router...	<p>CAUSE: This phone is proceeding through boot-up.</p> <p>RESOLUTION: Allow the phone to continue.</p>
Gatekeeper Error	<p>CAUSE: The gatekeeper rejects the registration attempt for an unspecified reason.</p> <p>RESOLUTION: Review gatekeeper and call server administrations, including IP network parameters.</p>

Table continues...

Message	Cause/Resolution
Gateway Error	<p>CAUSE: DEFINITY Release 8.4 does not have an H.323 station extension for this phone.</p> <p>RESOLUTION: On the station administration screen, ensure the DCP set being aliased for this IP phone has an H.323 station extension administered, in accordance with switch administration instructions. Since the IP phones are not supported on DEFINITY Release 8.4, you must upgrade to a release that supports these phones.</p>
Incompatible	<p>CAUSE: This release of the call server does not support the current version of the IP phone.</p> <p>RESOLUTION: Upgrade to the current version of Communication Manager (3.0 or greater) software.</p>
Invalid file	<p>CAUSE: The phone does not have sufficient room to store the downloaded file.</p> <p>RESOLUTION: Verify that the proper filename is administered in the script file, and the correct application file is located in the appropriate location on the HTTP or HTTPS server.</p>
IP address Error	<p>CAUSE: The gatekeeper reports an invalid IP address.</p> <p>RESOLUTION: This must not happen. Contact Avaya support.</p>
License Error	<p>CAUSE: The call server does not support IP telephony.</p> <p>RESOLUTION: Contact Avaya to upgrade your license.</p>
Limit Error	<p>CAUSE: The call server has reached its limit of IP stations.</p> <p>RESOLUTION: Un-register phones that are not in use, or contact Avaya to upgrade your license.</p>
NAPT Error	<p>CAUSE: A device between the phone and the call server is invoking Network address Port Translation (NAPT), which the phone do not support.</p> <p>RESOLUTION: Contact the System Administrator to remove or re-administer the device.</p>
No Ethernet	<p>CAUSE: When first plugged in, the IP phone is unable to communicate with the Ethernet.</p> <p>RESOLUTION: Verify the connection to the Ethernet jack, verify if the jack is Category 5, verify if power is applied on the LAN to that jack.</p>
Packet Error	<p>CAUSE: Protocol timeout error.</p> <p>RESOLUTION: Reenter the correct extension and password. If the condition persists, contact the system administrator.</p>
Password Error	<p>CAUSE: The call server does not recognize the password entered and displays the <i>Login Error</i> screen.</p> <p>RESOLUTION: Confirm whether the password is correct, then try registering again, and enter the password accurately.</p>

Table continues...

Message	Cause/Resolution
Request Error	<p>CAUSE: The gatekeeper does not accept the registration request sent by the phone as the request is not formatted properly.</p> <p>RESOLUTION: The phone will automatically attempt to register with the next gatekeeper on its list. If the problem persists, reboot the phone.</p>
Restarting...	<p>CAUSE: The phone is in the initial stage of rebooting.</p> <p>RESOLUTION: Allow the phone boot process to continue.</p>
Subnet conflict * to program	<p>CAUSE: The phone is not on the same VLAN subnet as the router.</p> <p>RESOLUTION: Press star (*) to administer an IP address on the phone. For information on configuring an IP address, see administer network equipment to administer the phone appropriately.</p>
System busy	<p>CAUSE: Most likely, the number of IP endpoints on the call server is already at maximum capacity. Network resource may not be unavailable.</p> <p>RESOLUTION: The phone attempted to access a network resource such as DHCP server, HTTP server, or the call server and was not successful. Check the resource being called upon for its availability. If the resource appears operational and is properly linked to the network, verify that the addressing is accurate and that a communication path exists in both directions between the phone and the resource.</p>
System Error	<p>CAUSE: The call server has an unspecified problem.</p> <p>RESOLUTION: Consult your Avaya Media Server administration and troubleshooting documentation.</p>
Undefined Error	<p>CAUSE: The call server has rejected registration for an unspecified reason.</p> <p>RESOLUTION: Consult your Avaya Media Server administration and troubleshooting documentation.</p>
Updating: DO NOT UNPLUG THE phone	<p>CAUSE: The phone is updating its software image.</p> <p>RESOLUTION: The phone update process must be continued.</p>
Waiting for LLDP	<p>CAUSE: No File Server or Call Server has been administered, so the phone is expecting to get the missing data through LLDP.</p> <p>RESOLUTION: Administer the missing data by one of the following methods: Statically, dynamically in DHCP, in the 46xxsettings file for Call Server addresses, or by LLDP.</p>
Wrong Set Type	<p>CAUSE: The call server does not recognize the set type.</p> <p>RESOLUTION: Ensure the call server is properly administered to register a compatible phone for the IP address and extension.</p>

Operational errors and status messages

The following table identifies some of the possible operational problems that might be encountered after successful phone installation. The user guide for a specific phone model also contains

troubleshooting for users having problems with specific IP phone applications. Most of the problems reported by phone users are LAN-based, where Quality of Service, server administration, and other issues can impact end-user perception of IP phone performance.

Table 23: Operational error conditions

Condition		Cause/Resolution
The phone continually reboots, or reboots continuously about every 15 minutes.		<p>CAUSE: The phone cannot find the HTTP/HTTPS server and/or call server.</p> <p>RESOLUTION: Ensure that MCIPADD is administered either manually or through DHCP or HTTP, as appropriate. Alternately, this might be a firmware fault because the MAC address in memory is corrupted; in this case, you must return the phone to Avaya for repair.</p>
The message light on the phone turns on and off intermittently, but the phone never registers.		<p>CAUSE: This is a hardware fault.</p> <p>RESOLUTION: You must return the phone to Avaya for repair.</p>
The phone stops working in the middle of a call,	AND no lights are lit on the phone and the display is not lit.	<p>CAUSE: Loss of power.</p> <p>RESOLUTION: Check the connections between the phone, the power supply, and the power jack. For example, verify whether static addressing was not used or that any changes to static addresses were entered correctly. Follow POE guidelines to troubleshoot POE related problems.</p>
	AND power to the phone is normal and the phone might have gone through the restarting sequence.	<p>Loss of path to the Avaya call server, expiry of DHCP lease, or unavailable DHCP server when telephone attempts to renegotiate DHCP lease.</p> <p>RESOLUTION: As above.</p>
The phone was working, but does not work now,	AND no lights are lit on the phone and the display is not lit.	<p>CAUSE: Loss of power.</p> <p>RESOLUTION: Check the connections between the phone, the power supply, and the power jack. Follow POE guidelines to troubleshoot POE related problems.</p>

Table continues...

Condition		Cause/Resolution
	AND power to the phone is normal, but there is no dial tone. The display might show "System Busy."	<p>CAUSE: Loss of communication with the call server.</p> <p>RESOLUTION: Check LAN continuity from the call server to the phone using ARP or trace-route and from the phone to the call server by invoking a Feature button. Verify that LAN administration has not changed for the Gatekeeper, TN 2302AP boards, or the LAN equipment (routers, servers, etc.) between the switch and the phone.</p> <p>Verify that telephone settings are not changed locally using VIEW and ADDR information, as described earlier in this guide. Verify that the telephone volume is set high. Finally, conduct a self-test.</p>
	AND the phone was recently moved.	<p>CAUSE: Loss of communication with the call server.</p> <p>RESOLUTION: As above, but verify whether the phone is being routed to a different DHCP server, or even a different call server switch. If so, the new server or switch might need to be administered to support the phone.</p>
	AND the network was recently changed to upgrade or replace servers, re-administer the Avaya Media Server, add or change NAT, etc.	<p>CAUSE: Loss of communication with the call server.</p> <p>RESOLUTION: As above.</p>
The phone works, but the audio quality is poor, specifically:		
	the user hears echo when speaking on a handset.	<p>CAUSE: Echo from digital-to-analog conversion on your Avaya Media Server trunk.</p> <p>RESOLUTION: Identify the trunk that is causing the echo, and swap the Trunk Termination parameter for that trunk on the call server.</p>
	the user hears an echo on a headset, but not on a handset.	<p>CAUSE: Improper headset cord.</p> <p>RESOLUTION: Ensure that an headset cord approved by Avaya is being used.</p>
	the user is on Speaker and hears no echo, but the far-end hears echo.	<p>CAUSE: Room acoustics.</p> <p>RESOLUTION: Ensure that there are six inches or so of blank space to the right of the phone. If that is insufficient, use the handset.</p>

Table continues...

Condition		Cause/Resolution
	the user experiences sudden silences such as gaps in speech, or static, clipped or garbled speech, etc.	<p>CAUSE: Jitter, delay, dropped packets, etc.</p> <p>RESOLUTION: You can have the user provide diagnostic data to Avaya support by invoking the Network Information feature under the A (Avaya Menu) or Home button on the phone. One or more Quality of Service (QoS) features should be implemented in the network.</p> <p>CAUSE: Improper non-Category 5 wiring.</p> <p>RESOLUTION: Replace non-Category 5 wiring with Category 5 wiring.</p>
	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.	<p>CAUSE: The user has changed the Automatic Gain Control (AGC) or environmental acoustics are not consistent with the current audio settings.</p> <p>RESOLUTION: Try different <i>On</i> or <i>Off</i> settings for the AGCHAND, AGCHEAD, and AGCSPKR parameters.</p>
The phone works properly except for the Speaker.		<p>CAUSE: The Speaker was turned off at the call server.</p> <p>RESOLUTION: Administer the call server to allow that station's Speaker to operate. If that does not work, do a self-test on the phone.</p>
The phone works properly, but you cannot hear incoming DTMF tones.		<p>CAUSE: The TN2302AP board does not pass in-band DTMF tones.</p> <p>RESOLUTION: None; the board is operating as designed.</p>
The phone works properly, but you cannot hear incoming DTMF tones.		<p>CAUSE: Call server suppresses sidetone DTMF.</p> <p>RESOLUTION: After completing call server administration, enable On-Hook Dialing on the Change-System-Parameters screen. If the user has enabled Hands-Free Answer (HFA), answers a call using the Speaker, switches to the handset, and presses dialpad buttons, the phone does not transmit DTMF tones. Disable HFA to hear DTMF tones.</p>
Hands-Free Answer (HFA) is administered but the phone did not automatically answer a call.		<p>CAUSE: HFA only works if the phone is idle. The phone ignores a second call if a call, including the ringing tone is in progress.</p> <p>RESOLUTION: None.</p>

Table continues...

Condition		Cause/Resolution
The phone does not use and ignores the HTTP or HTTPS script file and settings file.		<p>CAUSE: The system value AUTH is set to 1 which indicates that HTTPS is required but no valid address is specified in TLSSRV.</p> <p>RESOLUTION: Change AUTH to 0 (zero), or enter a valid address for TLSSRV.</p>
The HTTP or HTTPS script file is ignored or not used by the phone,	AND the HTTP or HTTPS server is a LINUX or UNIX system.	<p>CAUSE: The phone expects lines of the script file to terminate with a <Carriage Return> <Line Feed>. Some UNIX applications only terminate lines with <Line Feed>. Editing the script file with a UNIX-based editor can strip a <Carriage Return> from the file. Doing so causes the entire file to be treated as a comment, and thus be ignored.</p> <p>RESOLUTION: Edit the script file with a Windows® — based editor, or another editor that does not strip out the <Carriage Return>.</p> <p>CAUSE: UNIX and LINUX systems use case-sensitive addressing and file labels.</p> <p>RESOLUTION: Verify the file names and path in the script file are accurately specified.</p>
	AND phone administration recently changed.	<p>CAUSE: The 96xxupgrade.txt file was edited incorrectly, renamed, etc.</p> <p>RESOLUTION: Download a clean copy of the 96xxupgrade.txt file from the Avaya support web site at http://www.avaya.com/support, and do not edit or rename the file. Customize or change <i>only</i> the 46xxsettings.txt file as required.</p>
The system ignores some settings in the settings file while other settings are being used properly.		<p>CAUSE: Improper administration of settings file.</p> <p>RESOLUTION: Verify that customized settings are correctly spelled and formatted.</p>
The system ignores some settings in the settings file while other settings are being used properly,	AND the setting being ignored is one or more of the AGC settings.	<p>CAUSE: The user changed the AGC settings, which were placed in the backup or restore file of the user.</p> <p>RESOLUTION: The user can reset the AGC values back to the required settings, or the backup file can be edited to delete the custom AGC settings.</p>
Telephone power is interrupted while the phone is saving the application file and the HTTP/HTTPS application stops responding.		<p>CAUSE: The HTTP or HTTPS server stops responding if power is interrupted while a phone is saving the application file.</p> <p>RESOLUTION: Restart the phone.</p>

Table continues...

Condition		Cause/Resolution
The user indicates an application or option is not available.		<p>CAUSE: The <code>46xxsettings.txt</code> file script is not pointed to accurately, or is not properly administered to allow the application.</p> <p>RESOLUTION: Verify that the <code>46xxsettings.txt</code> file script is properly specified for your system, verify that the file server is UNIX or LINUX, and verify the extension.</p> <p>Then verify that all the relevant parameters are accurately specified in the <code>46xxsettings.txt</code> file.</p>
User data disappeared when the user logged out of one phone and logged in to another phone.		<p>CAUSE: The second phone is unable to gain access to the backup file.</p> <p>RESOLUTION: Verify that the first phone creates a backup file.</p> <p>Then verify that the second phone is administered to retrieve data from the same location as the first phone.</p> <p>Ensure that all the relevant parameters are accurately specified as in the <code>46xxsettings.txt</code> file.</p> <p>Finally, verify that the HTTP and HTTPS server on which the backup file is located is operational and accessible from the second phone.</p>
The user reports that button module buttons are not labeled properly.		<p>CAUSE: Improper administration on the call server.</p> <p>RESOLUTION: Verify correct administration.</p>
The user reports that personalized labels cannot be placed on the button module's buttons,	AND the user has tried using the Program AD button feature.	<p>CAUSE: Improper administration on the call server.</p> <p>RESOLUTION: Verify correct administration.</p>
	AND the user has tried using the Personalize Labels option on the phone.	<p>CAUSE: The user pressed the button module button to indicate which button to relabel.</p> <p>RESOLUTION: The user should use the list displayed on the phone, scroll to highlight the desired button label, and press either OK or the corresponding line button.</p>

LLDP Troubleshooting

If the *Waiting for LLDP* message appears for more than a few seconds, the message generally indicates a problem with getting a value for the call server IP address. This error can occur due to incorrect settings in script files or in the way the network is configured.

On booting, the phone must obtain a valid IP address for the call server. The phone can obtain the value, known as MCIPADD, from several sources:

- A static or manually programmed address on the phone.
- The 46xxsettings.txt file MCIPADD setting.
- A DHCP offer using option 242 that includes the MCIPADD setting.
- Link Layer Discovery Protocol or *LLDP*.

If the phone cannot find MCIPADD through any of these means, it will fail to register with the Call Server and will display the *Waiting for LLDP* message several times before rebooting. For example, if the MCIPADD value was specified in the 46xxsetting file and the network file server fails, the phone will not be able to read the MCIPADD value or any of the 46xxsettings file parameters. Therefore, do not use this method of providing MCIPADD.

Proposed Solution

Procedure

1. A more robust way to provide this value is to use DHCP. You can administer the DHCP server to provide MCIPADD using DHCP Option 242. You can also administer the TLSSRV, HTTPSRV and L2QVLN parameters using this option. phones using non-static addressing automatically use the DHCP request method. Option 242 is the default DHCP offer and may get MCIPADD and other addresses using this way.
2. The phone displays the *Waiting for LLDP* message when both the HTTP and HTTPS Server IP address are not administered. To administer the HTTP and/or HTTPS server, use the Craft ADDR procedure and enter the correct HTTP and or HTTPS File Server IP address in the File Server field.
3. An alternative protocol known as LLDP can also supply call server, and file server with HTTP and HTTPS IP addresses. This IETF standard protocol requires the network to be equipped and configured to support LLDP. You can provide HTTP and the HTTPS Server and call server IP addresses with LLDP in the network using proprietary Transport Layer Values (TLVs) to pass information to the phones.

LLDP setup and troubleshooting steps

Note:

If system value *STATIC* is set to 0 which is the default setting, the DHCP or the 46xxsettings file might overwrite the static addresses.

Proposed solution for DHCP configured deskphones

Procedure

1. Using the Craft *ADDR* procedure, set *Phone* to **0.0.0.0**.
2. Verify or set *SSON* to **242** which is the default value.
3. Administer the DHCP server option 242 to include **MCIPADD=xxx.xxx.xxx.xxx** where xxx.xxx.xxx.xxx is the call server IP address.
4. Verify that the DHCP server and the deskphone are on the same VLAN.
5. Verify the *DHCP server* port 67 and or the *DHCP client* port 68 are not blocked on the switch.
6. Verify the configuration of the DHCP Relay Agent on the switch or on a separate PC, for example, MS Windows Server 2000/2003 whether the deskphones and DHCP Server are placed on different networks or subnets. DHCP broadcast messages do not, by default, cross the router interface.

Proposed solution for script-configured deskphones

Procedure

1. Edit the 46xxsettings.txt file to contain a valid Call Server IP address with the line **SET MCIPADD xxx.xxx.xxx.xxx** where xxx.xxx.xxx.xxx is the Call Server IP address.
2. Verify that the 96xxupgrade.txt file contains the line **GET 46xxsettings.txt** as the last command line of the upgrade file.
3. Verify that the deskphone can reach the HTTP server and whether the HTTP server is activated.
4. Verify that the 96xxupgrade.txt and 46xxsettings.txt files are placed in the proper directory of the HTTP server to access these files.

Proposed solution for LLDP-configured deskphones

About this task

For LLDP-configured deskphones, activate the switch the deskphone is connected to for LLDP. This is currently only possible with Extreme switches. Activating the switch for LLDP enables the switch to send appropriate IP addresses using Avaya/Extreme Proprietary HTTP and/or HTTPS Server and/or Call Server TLVs.

 **Note:**

The deskphone obtains the HTTP and or HTTPS Server and Call Server IP addresses from LLDP only if the addresses were not configured through other means such as DHCP Server, Script File, or statically.

*** Note:**

Set the switch LLDP repeat timer to less than 30 seconds.

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*

Secure Shell Support

The phone supports the Secure Shell (SSH) v2 protocol. The SSH protocol is a tool that the Avaya services organization can use to remotely connect to IP deskphones to monitor, diagnose, or debug deskphone performance. Because of the sensitive nature of remote access, you can disable permission with the SSH_ALLOWED parameter.

The deskphone displays a security warning message at start of the session. You can specify your own file using SSH_BANNER_FILE, or the deskphone will use the following default file:

```
This system is restricted solely to authorized users for legitimate
business purposes only. The actual or attempted unauthorized access,
```

use, or modification of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials. All users must comply with all corporate instructions regarding the protection of information assets.

The Avaya technician can match the SSH fingerprint displayed under debug with the fingerprint present in the SSH client. This information is used to verify whether the administrator is logged on to the correct SSH server. The SSH fingerprint is not displayed when the FIPS mode is enabled. The deskphones support 2048-bit asymmetric key length for SSH server.

You can also administer the `SSH_IDLE_TIMEOUT` parameter to configure the duration of inactivity that will disable SSH.

Troubleshooting Avaya J100 Expansion Module

Condition

Either of the following is observed:

- Avaya J100 Expansion Module display screen is dark.
- The expansion module lines are not displayed.
- The action on Avaya J100 Expansion Module does not cause the corresponding result on the phone.
- The action on the phone does not cause the corresponding result on Avaya J100 Expansion Module.
- After the upgrade or downgrade is completed, the connection to Avaya J100 Expansion Module is lost.

Solution

1. Check if the phone has the power supply.
2. Check if Avaya J100 Expansion Module is attached to the phone correctly and the connection cable is not damaged.
3. Plug Avaya J100 Expansion Module connection cable out and in.
4. Reboot the phone. The expansion module will reboot automatically.
5. In Craft menu, check if the connection type is set to **Adjunct**.

Related links

[Debugging the expansion module](#) on page 265

Debugging the expansion module

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

*** Note:**

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

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

*** Note:**

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

! Important:

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

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

Command	Description
<code>help</code>	To print <code>bm_cli</code> help.
<code>create_authfile</code>	To install and activate <code>authfile.txt</code> . Specify the expansion module ID, for example: <pre>create_authfile 1</pre> <p>* Note:</p> <p>By default, the expansion modules are numbered in the order as they are connected to the phone, i.e.: 1, 2, 3.</p>
<code>get_file</code>	To retrieve the specified file. Specify the expansion module ID and the path for the file you want to retrieve, for example: <pre>get_file 1 "/AvayaDir/var/log/bm/avaya_phone.log.1.gz"</pre> <p>Use <code>-c</code> argument to activate GZIP compression.</p> <p>* Note:</p> <p>Add <code>/bm</code> to the file path as set in the example to ensure no empty files are created.</p>

Table continues...

Command	Description
<code>list_files</code>	To view the list of log files of the selected expansion module in the specified directory, for example: <code>list_files 1 "/AvayaDir/var/log"</code>
<code>remove_authfile</code>	To deactivate <code>authfile.txt</code> for the selected expansion module, for example: <code>remove_authfile 1</code>
<code>set_log_category</code>	To set a log category for the selected expansion module. * Note: The full list of available log categories and their description is provided in your <code>46xxsettings.txt</code> file. View allowed values for the <code>LOG_CATEGORY</code> parameter.
<code>set_log_level</code>	To set a log level for the selected expansion module, for example: <code>set_log_level 1 0</code> * Note: The full list of available log levels and their description is provided in your <code>46xxsettings.txt</code> file. View allowed values for the <code>LOCAL_LOG_LEVEL</code> parameter.

Related links

[Troubleshooting Avaya J100 Expansion Module](#) on page 264

Index

Numerics

46xxsettings	
JITC parameters	80, 216
reboot	228
802.1X	173
802.1X operational mode, setting	58
9600 Series IP Deskphone	
powering the	32

A

adjusting for button modules	233
adjusting for button modules or non-color ip deskphones	234
administering	193
DIFFSERV	100
guest user	208
input methods	180
language selection	180
QOS	100
RSVP	100
visiting users	
administering	208
VLAN	166
Administering Features	106
administration	
call server	99
checklist	72
DHCP and file servers	108
parameters	78, 214
responsibilities	71
administration,	73
Administration menu	
Administration menu after phone startup	54
Administrative Options	
Entering Data for	54
administrator	
responsibilities	71
agc	234
aliasing	107
application file	
upgrade script file	
application file	124
Application Status Flag (APPSTAT)	203
Application Status Flags and Their Meaning	203
APPSTAT	203
Audio equalization	193
Auto-answer	195
Auto Hold administration	104
automatic gain control, disable or enable	234
Auto select any idle appearance administration	106
Avaya	205
Avaya Menu Administration File Template	205

B

Backup	199
Backup, Options and Non-Password Parameters Saved ..	200
Backup/Restore	197
Backup/restore processing	118
Backup File Formats	199
button modules	
overview	23
wall mounting	50

C

calibrating the touch screen	232
Call Center faceplate installation (9641G)	42
call server	
administration	99
requirements	98
call servers	
IP interface and addresses	99
call transfer	
considerations	102
certificate, revocation	76, 212
certificates	76, 212
certificates, OCSP	76, 212
certificates, revocation	76, 212
certificates, security	76, 212
certificates, usage	76, 212
Changing the Signaling Protocol	231
checklist	
initial administration	72
post installation	70
clear settings	
phone administration	
clear settings	61
Conference/Transfer on Primary Appearance administration	106
connecting the deskphone	37
considerations during call conferences	102
contrast	233, 234
Coverage Path administration	104, 106
craft menu	54
craft procedure	248
craft procedures	
running	53
customizable options	126
custom screen saver, administering	192

D

data precedence	
parameters	74, 210
deployment process	

deployment process (<i>continued</i>)	
initial setup and connectivity	31
device upgrade	222
DHCP	
generic setup	
DHCP	109
DHCP, Parameters Set by	113
DHCP Generic Setup	113
DHCP options	109 , 116
DHCP server	87
dialing methods	182
DIFFSERV	
administering	100
Disable Event Logging	64
disable or enable automatic gain control	234
display	
secondary	23
DNS addressing	168
document changes	11
download and save the software	222
Downloading Text Language Files	231
downloads	
certificate files	75 , 211
language files	75 , 211
settings configuration files	75 , 211
upgrade configuration files	75 , 211
DTMF Tones	247
Dual Headset Adapter, installing	37
dynamic addressing process	43
E	
EAP-TLS	168
authentication	169
phones using MD5	170
scenarios	170
without 802.1 authentication	172
EASG	97
EC500 administration	104
enable automatic gain control	234
Enable Event Logging	64
enabling	
SCEP support	168
Enhanced Conference Features administration	104 , 106
Entering Data for Administrative Options	54
error conditions	85 , 221
Error Conditions	247
error messages	251
Event Logging	64
expansion module	
generating log files	265
troubleshooting	264
upgrade overview	224
upgrading	225

F

faceplate installation, for 9641G use in call center	42
Far End Mute administration	106
Feature administration for all other deskphones	107
Feature Administration for Avaya Communication Manager	104
Feature Numbers for Assigning Softkeys	185
Feature-Related System Parameters, administering on CM	104
Files	
configuration	75 , 211
settings	
language	75 , 211

G

General Download Process	122
group identifier	236
GROUP parameter	125
GROUP Parameter	232

H

handset audio equalization	
setting	235
hardware dimensions	16 , 18
hardware requirements	86
Home screen	
managing applications	183
HTTP redirect	118

I

idle timer settings	208
IEEE 802.1D and 802.1Q	88
IEEE 802.1Q	100
IEEE 802.1Q QoS parameters	100
initialization process	74 , 210
initial setup and connectivity	
deployment process	31
phone setup	30
installation	
required network information	87
installing	
phone	25
Installing a Dual Headset Adapter	37
Interface Control	63
ip deskphones	28
IP deskphones	
customizing applications and options	203
IP interface and addresses	
call servers	99
IPv4 and IPv6 operation	120
IPv6	120

IPv6 Limitations	121	optional components	23
IPv6 operation		options	
DHCPv6 configuration	112	local administrative	179
K		options, customizing	203
knowledge	26	overview	13
		JITC security	79 , 215
L		P	
Language Files for text entry, Downloading	231	parameter	194
Link Layer Discovery Protocol (LLDP)	175	parameters	
LLDP troubleshooting	260	administration options	78 , 214
local administrative		data precedence	74 , 210
options	179	parameters, customizable	127
Local administrative procedures	57	parameters in real-time	89
local craft procedures	52	Parameters Saved During Backup	200
Logging in to your phone extension	71	phone	
logoff procedure	65	administration	104
LOG Procedure	64	call server initialization	77 , 213
		file server initialization	75 , 211
M		initialization to DHCP server	75 , 211
maintenance		network initialization	75 , 211
manual upgrade	223	restarting	67
Maintenance		wall mounting	48
downloading text language files	224	phone model	14 , 15
manual		phone setup	
upgrade files	223	initial setup and connectivity	30
mode, JITC	79 , 215	port selection	
		UDP	99
N		powering	32
NAT	100	power interruption	248
network assessment	85	power management	20
network considerations		Power management	22
audio quality display	89	power-up and reset process	43
generic setup		pre-installation checklist	28
DHCP	88	preinstallation data gathering	27
IP address	88	prerequisites	
IP address lists	89	hardware	26
ping	88	software	26
port utilization	90	protection	
QoS	88	acoustic protection	194
quality of service	88	purpose	11
SMLv2	87	Q	
SNMP	87	QoS	
Station Number Portability	89	administering	100
TCP/UDP	90	IEEE 802.1Q	100
Time-to-Service (TTS)	97	R	
traceroute	88	Registration and Authentication	96
O		required network information	87
Onhook Dialing on Terminals	104	requirements	28
operation errors	255	call server	98
		hardware	86

requirements (<i>continued</i>)	
server	86
resetting the phone	43
reset values	
phone administration	
reset values	66
Restore	201
Restore/Backup	197
Restrict Last Call Appearance administration	106
RSVP	
administering	100

S

SCEP support	
enabling	168
screen saver, administering	192
Secure Shell Support	96 , 263
security	94
security, compliance	79 , 215
security, FIPS	79 , 215
self-test	69
Send All Calls (SAC) administration	106
server	
requirements	86
settings file	124
settings file, contents	227
Signaling Protocol, Changing	231
Signaling Protocol Identifier	67
SIG Procedure	67
Site-Specific Option Number Setting	68
skills	26
SLA Mon™ agent	263
SNMP	
enablement	87
Softkeys, Administering Features on	185
software	
downloading and saving	222
Software	31
software distribution packages	225
software prerequisites	107
software upgrades	225
S RTP	90
SSO logon	165
SSON, Option 242, configuring	113
SSON Procedure	68
station administration	106
Station Form Administration Results Chart	107
Station Number Portability	
IP address lists	89
status messages	251 , 255
supplicant operation, 802.1X	174
switch compatibility and aliasing IP telephones	107
System Parameters	104
system parameters, customizable	127

T

TLS	90
tools	26
touch screen, calibrating	232
troubleshooting	248
DTMF tones	247
power interruption	248
Troubleshooting	
Error Conditions	247
troubleshooting LLDP	260

U

UDP	
port selection	99
UDP/TCP Port Utilization	90
unnamed registration	47 , 77 , 213
upgrade	
manual	223
upgrading	124

V

VLAN	
administering	166
VLAN Default Value	166
VLAN detection	167
VLAN tagging	166

W

wall mounting	48
Wideband Audio administration	104
WML browser	184
WML browser properties	184