Administering Avaya 9608/9608G/9611G/ 9621G/9641G/9641GS IP Deskphones H. 323

Release 6.6.5
Issue 2
March 2018

Note

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Regulatory Statements

Japan Statements

Class B Statement

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

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

Denan Power Cord Statement

Danger:

Please be careful of the following while installing the equipment:

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

警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

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

México Statement

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

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

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

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

Power over Ethernet (PoE) Statement

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

EU Countries

General Safety Warning

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction 8
Introduction 8
Purpose 8
Related resources 8
Support 9
Chapter 2: 9600 Series IP deskphone overview 10
Overview of the 9600 Series IP Deskphones 10
Administrator responsibilities 10
Initial administration checklist 11
Chapter 3: Administration overview and requirements 14
Administration overview and requirements 14
Administrative requirements 14
Parameter data precedence 15
Initialization process overview 15
JITC security compliance mode overview 19
Aliasing deskphones for switch compatibility 25
Error conditions 25
Chapter 4: Network requirements 26
Network requirements 26
Network assesment 26
Hardware requirements 26
Server requirements 27
Required network information 27
Other network considerations 28
Chapter 5: Communication Manager Administration 39
Communication Manager Administration 39
Call server requirements 39
Call server administration 39
Administering Voice mail 42
Call transfer administration 43
Call conferencing 44
Administering deskphones on Avaya Aura® Communication Manager 45
Station administration 47
Administering features and CAs for all other IP deskphones 48
Chapter 6: Server Administration 50
Server Administration 50
Software prerequisites 50
Administering the DHCP and file servers 50
DHCP generic setup 51

Setting up the DHCP server ... 52
Setting up a DHCPv6 server ... 58
HTTP generic setup ... 58
Backup and restore processing ... 60
About IPv4 and IPv6 operation ... 62
Features not supporting IPv6 ... 64
Chapter 7: Telephone software and application files ... 65
Telephone Software and Application Files ... 65
Understanding the general download process ... 65
Using the GROUP parameter to set up customized groups ... 68
Chapter 8: Administering Deskphone Options ... 70
Administering Deskphone Options ... 70
Administering options for 9600 Series H.323 Deskphones ... 70
9600 Series H.323 customizable system parameters ... 71
Single Sign on for local devices (SSON-LD) ... 101
Administering a VLAN ... 102
About DNS addressing ... 104
EAP-TLS support for authentication ... 105
About IEEE 802.1X ... 110
About Link Layer Discovery Protocol (LLDP) ... 112
Administering settings at the phone ... 116
Administering display language options ... 117
Administering dialing methods ... 118
About internal audio parameters ... 118
Managing applications on the Home screen ... 119
Administering features on softkeys ... 122
Administering a custom screen saver ... 130
About administering audio equalization ... 130
Administering deskphones for call center operation ... 131
Ringing on wireless headset ... 132
Configuring phone based auto-answer ... 133
Administering backup and restore ... 135
Chapter 9: Administering Applications and Options ... 142
Administering Applications and Options ... 142
Customizing Applications and Options ... 142
Setting the Application Status flag ... 143
Administering the Avaya A Menu ... 145
Special Administration for Touchscreen Deskphones ... 146
Administering WML applications on the Avaya Menu ... 146
Administering the Avaya Menu with WML applications ... 147
How the Home screen displays WML applications ... 149
Sample Avaya Menu Administration File Template ... 152
Administering guest users ... 154

Administering visiting users 154
Idle timer configuration..... 155
Glossary..... 157

Chapter 1: Introduction

Introduction

Purpose

The purpose of this guide is to provide instructions on installation, deployment, initial administration, maintenance, and troubleshooting for 9600 Series H.323 Deskphones.

This guide is intended for personnel who install, administer, and maintain Avaya Aura® Communication Manager, DHCP, and HTTP/HTTPS servers for Avaya 9608, 9608G, 9611G, 9621G, 9641G, and 9641GS IP Deskphones H.323, and a Local Area Network (LAN). All models except the 9608 have a Gigabit Ethernet switch with which the phone and a PC can share the same LAN connection. Thus, these models do not work with the 30A switched hub interface. The 9641G and 9641GS deskphones also have an integrated Bluetooth™ interface. For information about setting up a Bluetooth™ device, see the *Using Avaya 9621G/9641G/9641GS IP Deskphones H.323* guide.

This document describes the installation and maintenance procedures for the deskphones. For information about using the deskphone features, see the user documentation. For information about desk mounting or wall mounting, see the instructions boxed with the phone or the Avaya Support website at https://support.avaya.com/.

Related resources

Documentation

For more information related to the use of the H.323 9600 IP Deskphones refer the following documents available at support.avaya.com:

Document number	Title	Use this document to:	Audience
Overview			
16-604299	*Avaya 9600 Series H.323 IP Deskphones Overview and Specifications*	Refer to the overview and specifications.	People who want to gain a high-level

Table continues…

Document number	Title	Use this document to:	Audience
			understanding of the product features, functions, capacities, and limitations.
Using			
16–603593	*Using Avaya 9608, 9608G, and 9611G IP Deskphone H. 323*	Refer to tasks related to using the deskphone.	End users and administrators
16–603594	*Using Avaya 9621G/9641G/ 9641GS IP Deskphones H.323*	Refer to tasks related to using the deskphone.	End users and administrators
16-603613	*Using Avaya 9608/9608G/ 9611G/9621G/ 9641G/9641GS IP Deskphones H.323 for Call Center Agents*	Refer to tasks related to using the deskphone in a call center environment.	End users and administrators
Implementing			
16–603603	*Installing and Maintaining Avaya 9608/9608G/9611G/ 9621G/9641G/9641GS IP Deskphones H.323*	Refer to procedures related to installing and upgrading the deskphone.	Administrators

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field and click **Go** to search the course.

Course Code	Course Title
ACIS-6002 ACIS	Avaya Aura® Communication Manager and CM Messaging - Embedded (R6.x)
APSS-1300 APSS	Avaya Networking Solutions

Support

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

Chapter 2: 9600 Series IP deskphone overview

Overview of the 9600 Series IP Deskphones

Avaya 9608, 9608G, 9611G, 9621G, 9641G, and 9641GS IP deskphones use Internet Protocol (IP) technology with Ethernet line interfaces and support both H.323 and SIP protocols. These deskphones support DHCP, HTTP, and HTTPS to obtain customized settings and to download new versions of software for the deskphones.

All 9600 Series IP Deskphones currently support the H.323 signaling protocol.

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:

Avaya does not support many of the products mentioned in this document. Ensure that adequate technical support is available for servers used with any 9600 Series IP Deskphones system. If the servers do not function correctly, the deskphones will not operate correctly.

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

For more information on using the 9600 Series IP Deskphones in an IP Office environment, see the Avaya support site at http://support.avaya.com/css/P8/documents/100150378.

Administrator responsibilities

To administer the 9600 Series IP Deskphones, complete the tasks in the order shown.

1. Administer the switch for 9600 Series IP Deskphones.

2. Administer LAN and applicable servers to accept the deskphones.
3. Download the deskphone software from the Avaya support site.
4. Update the 46xxsettings file with site-specific information, as applicable.
5. Install 9600 Series IP Deskphones. For more information, see *Installing and Maintaining Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*,16-603603 covering the 9608, 9611G, 9621G, 9641G, and 9641GS deskphones, and *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694* for all other 9600 Series IP Deskphones models.
6. Update each 9600 Series IP Deskphones using Craft procedures, as applicable. For more information about local administrative procedures, see *Installing and Maintaining Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*.

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 1: 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 26.	
2	Install the license for call server.	-	Communication Manager Administration on page 39.	
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	Vendor-provided instructions.	

Table continues…

#	Task	Description	Related information	✔
		computer that is connected to the LAN.		
7	Download the following files: • Application files • Script file • Settings file	Download the files from the Avaya support site.	www.avaya.com/support Telephone Software and Application Files on page 65.	
8	Edit the Settings file.	Use your own tools to edit the settings file as required.	Telephone Software and Application Files on page 65.	
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.	*Avaya IP Deskphone Edition for 9600 IP Telephones Application Programmer Interface (API) Guide, 16-600888*	
10	Local administration of deskphones as applicable	As a Group:	Using the GROUP parameter to set up customized groups on page 68 and the *Installing and Maintaining Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*, 16-300694 for all, but Release 6.2 and Document Number 16-603603 for Release 6.2 covering the 9608,9608G, 9611G, 9621G, and 9641G deskphones.	
		Individually:	The applicable Craft Local Procedures in the *Installing and Maintaining Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*,	

Table continues…

#	Task	Description	Related information	✔
			Document Number 16-300694 for all, but Release 6.2 and Document Number 16-603603 for Release 6.2 covering the 9608,9608G, 9611G, 9621G, and 9641G deskphones.	
11	Phones installation in the network	-	*Installing and Maintaining Avaya 9608/9608G/9611G/ 9621G/9641G/ 9641GS IP Deskphones H.323*, Document Number 16-300694 for all, but Release 6.2 and Document Number 16-603603 for Release 6.2 covering the 9608, 9608G, 9611G, 9621G, and 9641G deskphones)	
13	User modification of Options, if applicable	-	OPSTAT and the respective User Guide for the specific deskphone model.	
14	VPN functionality administration if applicable	Enable or disable VPN, provide administration for your particular VPN environment.	*VPN Setup Guide for 9600 Series IP Telephones*, 16-602968	

Chapter 3: Administration overview and requirements

Administration overview and requirements

Administrative requirements

This topic outlines the operating environment for the 9600 Series IP deskphones as follows:

- Deskphone Administration on the Avaya call server.
- IP address management for the deskphone.

  For more information about static addressing, see *Installing and Maintaining Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*,16-603603 covering the 9608, 9611G, 9621G, 9641G, and 9641GS deskphones, and*Avaya IP Deskphone Edition for 9600 Series IP Telephones. Installation and Maintenance Guide*, 16-300694 for all other 9600 Series deskphone models.
- 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.

  For more information, see, *Installing and Maintaining Avaya 9608/9608G/9611G/9621G/ 9641G/9641GS IP Deskphones H.323*,16-603603 covering the 9608, 9611G, 9621G, 9641G, and 9641GS deskphones, and, *Avaya IP Deskphone Edition for 9600 Series IP Telephones. Installation and Maintenance Guide*,16-300694 for all other 9600 Series deskphone models.
- Application-specific phone administration, if applicable.

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 52.
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.

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

Connection to network on page 15
DHCP processing on page 16
File downloads on page 16
Certificates usage on page 16
Registration with the call server on page 17

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 15

DHCP processing

If an IP address has not been manually configured in the phone, the phone initiates DHCP, as described in Administering the DHCP and File Servers on page 50. Among other data passed to the phone is the IP address of the HTTP or HTTPS server.

Related links

Initialization process overview on page 15

File downloads

9600 Series IP Deskphones use the HTTP server to download the firmware, the language files, and the certificate files. The HTTPS server is used to download configuration files, and to backup or restore user information. The phone first downloads an upgrade, configuration file to identify the latest software files. Then, the phone downloads a settings, configuration file to identify the required language files and/or certificate files. Finally, the phone downloads software files depending on the software in the phone and if it is the same as that specified in the upgrade file. For more information about the download process and settings file, see Telephone Software and Application Files on page 65.

Related links

Initialization process overview on page 15

Certificates usage

The H.323-based 9600 Series IP Deskphones 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 15
Certificate revocation on page 16

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` 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 16

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` 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 15

Other administrable options using parameters on page 18

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 9600 Series IP Deskphones 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. The H.323 over TLS profile is not supported.

  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 17

JITC security compliance mode overview

The Avaya 9600 Series IP Deskphones H.323 firmware Release 6.6 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
- USB profile
- 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

JITC security compliance mode configuration on page 20

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` 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	Restricts the use of the default administration password of the deskphone. The value can be set on Communication Manager, DHCP server, or file server. **Note:** Obtaining PROCPSWD through Communication Manager is the most secure method. Setting PROCPSWD using HTTPS is secure only if mutual certificate authentication is done.
PKCS12URL	URL of the PKCS #12 file	The PKCS #12 file contains an identity certificate for the

Table continues…

Parameter	Value	Description
		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.
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	Specifies whether OCSP is used to verify the revocation status of the certificates. Valid values are: • 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. **Note:** H.323 over TLS, Backup/ restore, and file downloads are the only applications supported in the secured mode. 802.1x EAP-TLS,

Table continues…

Parameter	Value	Description
		SLA Mon, IPsec, VPN, and SSO are not supported.
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: • 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	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.

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. **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.
SNMPSTRING	NULL	9608, 9608G, 9611G, 9621G, 9641G do not support 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

Table continues…

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

Table continues…

Parameter	Value	Description
VUMCIPADD	NULL	Disables the visiting user login.

Related links

JITC security compliance mode overview on page 19

Aliasing deskphones for switch compatibility

Avaya B189 Conference IP Phone is not supported natively by Avaya Aura® Communication Manager. You need to alias the conference phone as 9620 phone on Avaya Aura® Communication Manager.

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.

For the likely operational problems after you successfully install 9600 Series IP Deskphones, see *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694*. You can also see the user guides for specific deskphone models and applications.

Chapter 4: Network requirements

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. For more information, see Administering UDP port selection on page 40.

To use the 9600 Series IP deskphones to reach the network through a Virtual Private Network 15 (VPN), see*VPN Setup Guide for 9600 Series IP Telephones*, 16-602968.

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.
- 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.

To ensure that you administer the appropriate circuit packs on your server, see Communication Manager Administration on page 39.

Server requirements

You can configure three types of servers for 9600 Series IP Deskphones:

- DHCP server: Avaya recommends that you install a DHCP server and do not use static addressing. Install the DHCP server as described in Administering the DHCP and File Servers on page 50.
- HTTP or HTTPS server:Administer the HTTP or HTTPS file server as described in HTTP Generic Setup on page 58.
- Web and Push servers (optional): If users have access to corporate WML web sites, administer the deskphones as described in Server Administration on page 50. 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, 16-600888*.

While the servers listed provide different functions that relate to the 9600 Series IP Deskphones, 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 39, and the administration documentation for your call server. For parameters related to DHCP and file servers, see Server Administration on page 50.

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 9600 Series IP Deskphones 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. For more information about DNS, see DHCP Generic Setup on page 51 and DNS addressing on page 104.

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. See Server Administration on page 50.
- Edit the configuration file on the applicable HTTP or HTTPS file server. See Choosing the right application file and upgrade script file on page 66.

Other network considerations

SNMP enablement

The 9600 Series IP Deskphones 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 accepts 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. For more information, see Server Administration on page 50 and 9600 Series H.323 customizable system parameters on page 71.

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 9600 Series IP Deskphones 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, see *Administering Avaya Aura® 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. For information about QoS implications for the 9600 Series IP Deskphones, see Administering QoS on page 41.

All 9600 Series IP Deskphones provide some detail about network audio quality. For more information, see Network Audio Quality Display on page 30.

IEEE 802.1D and 802.1Q

For more information about IEEE 802.1D and IEEE 802.1Q and the 9600 Series IP Deskphones, see Administering IEEE 802.1Q on page 41 and Administering a VLAN on page 102. 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 9600 Series IP Deskphones while on a call. You can view this information on the Network Information screen. You can view the Network Information screen on most 9600 Series IP Deskphones button-based deskphones from the Avaya (A) Menu and select the **Network Information** option directly if available. You can also select **Phone Settings**, then select the **Network Information** option. On touch screen deskphones such as 9621G, 9641G, and 9641GS, you can gain access to the Home screen, then select **Settings**, then **Network Information**.

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 2: 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 9600 Series IP Deskphones . 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.

For details on administration of DHCP servers for lists of alternate call servers, router/gateways, and HTTP/HTTPS servers, see Server Administration on page 50.

For more information on DNS addressing, see DNS Addressing on page 104.

TCP/UDP Port utilization

9600 Series IP Deskphones 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. For more TCP/UDP port utilization information related to Communication Manager, see UDP Port Selection on page 40.

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.

For more information about parameters and settings, see Administering Options for 9600 Series H.323 Deskphones on page 70.

Table 3: Received packets (Destination = 9600 Series IP Deskphones)

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

Table continues…

Destination port	Source port	Use	UDP or 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
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	TCP

Table continues…

Destination port	Source port	Use	UDP or TCP?
		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.	

Note:

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

Table 4: Transmitted packets (Source = 9600 Series IP Deskphones)

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	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
TLSPORT	Any unused port number	TLS/SSL packets that the HTTP client of the phone transmits during startup	TCP
443 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

Table continues…

Destination Port	Source Port	Use	UDP or 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
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

Table continues…

Destination Port	Source Port	Use	UDP or TCP?
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 9600 Series IP Deskphones 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 9600 Series IP Deskphones that have WML Web applications support Transport Layer Security (TLS). The deskphone uses TLS to establish a secure connection to a HTTP server, in which the upgrade and settings file can reside. The 9600 Series IP Deskphones 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:

- WML browser using HTTPS
- 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 9600 Series IP Deskphones 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 9600 Series IP Deskphones 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 HTTP server, the deskphone will prompt you to enter the realm address. For information about configuring realm, see the instructions provided by your HTTP 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. For more information on these options, see Server Administration on page 50.

- Support signaling channel encryption.

  Note:

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

- Restrict the response of the 9600 Series IP Deskphones 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 9600 Series IP Deskphones support 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 9600 Series 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.

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.

9600 Series IP Deskphones 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

For more information, see the *Administering Avaya Aura® Communication Manager*, 03-300509.

Chapter 5: Communication Manager Administration

Communication Manager Administration

Related links

Call server requirements on page 39
Call server administration on page 39
Call transfer administration on page 43
Call conferencing on page 44
Administering deskphones on Avaya Aura Communication Manager on page 45
Station administration on page 47
Administering features and CAs for all other IP deskphones on page 48

Call server requirements

Before you perform administrative tasks, ensure that you have installed the proper hardware and your call server software is compatible with 9600 Series IP deskphones. Use the latest PBX software and IP phone firmware.

Related links

Communication Manager Administration on page 39

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*, 03-300509 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*, 555-233-504 for more information about switch administration for your network.

Related links

Communication Manager Administration on page 39
Administering the IP interface and addresses on page 40
Administering UDP port selection on page 40
Administering RSVP on page 40
Administering QoS on page 41
Administering IEEE 802.1Q on page 41
Administering DIFFSERV on page 41
Administering NAT on page 41

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* , 555-233-504.
- 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 39

Administering UDP port selection

You can administer the 9600 Series IP deskphones from the Avaya Communication Manager Network Region form to support UDP port selection. For information on specific port assignment diagrams, see *Installing and Maintaining Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*, 16-603603 for the 9608, 9611G, 9621G, 9641G, and 9641GS deskphones.

Also see *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694* for all other 9600 Series deskphone modules.

For information about Avaya Communication Manager implementation, see *Administration for Network Connectivity for Avaya Communication Manager, 555-233-504* 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 39

Administering RSVP

9600 Series Avaya IP deskphones support the Resource Reservation Protocol (RSVP) for IPv4 audio connections only.

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

For more information, see your Avaya server administration documentation and *Administration for Network Connectivity for Avaya Communication Manager*, 555-233-504.

Related links

Call server administration on page 39

Administering QoS

The 9600 Series IP deskphones support both IEEE 802.1D/Q and DiffServ.

Related links

Call server administration on page 39

Administering IEEE 802.1Q

The 9600 Series IP deskphones 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 9600 Series IP deskphones from the network through LLDP, or by appropriate administration of the DHCP or HTTP/HTTPS servers.

You can administer the IEEE 802.IQ 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*, 555-233-504.

For information on setting these parameters manually, see *Installing and Maintaining Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*, 16–603603, and *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694* for other 9600 Series deskphone models.

Related links

Call server administration on page 39

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. For more information on DiffServ values, see chapter on *Network Quality Administration* in *Administration for Network Connectivity for Avaya Communication Manager, 555-233-504.* Unless there is a specific need in your enterprise LAN, do not change the default values.

Related links

Call server administration on page 39

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*, 555-233-504 on the Avaya Support website.

Related links

Call server administration on page 39

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 39

Voice mail for deskphones aliased as 4600 Series IP Telephones

When native support does not apply, 9600 Series IP deskphones are aliased as 4600 Series IP telephones and run under CM Release 3.1 or later. In this case, use the settings 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.

On the settings 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.

For more information on the SET MSGNUM parameter, see 9600 Series H.323 customizable system parameters on page 71.

Note:

You can use MSGNUM only when you aliase 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 39

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 39

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 39

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 39
Feature-related system parameters on page 45

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 settings 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 settings 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	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

Table continues…

Name	Description
	appearance. Use the System Parameters Features form, page 6.
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 Mapping`**
Wideband Audio	Enable Wideband Audio, by using the **`Change IP codec`** 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 96xx IP phones. Calls that involve three or more parties, even if all parties use 96xx IP phones, do not use wide band. Calls between two 96xx IP phones where audio is terminated at a port network/ gateway (PN/GW) media resource will not use wideband. Ensure that G.722 is added to all codec-sets that can possibly be used between all regions on the IP-Network Regions form where 96xx IP phones exist. 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).

Table continues…

Name	Description
	For information on using the wideband codecs with the Communication Manager, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Related links

Administering deskphones on Avaya Aura Communication Manager on page 45

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 file for administration of specific groups of deskphones. For more information, see Using the GROUP parameter to set up customized groups on page 68. You can administer the GROUP ID parameter on page 3 of the Change Station Form.

If applicable, before administering stations ensure that the deskphones are aliased according to the chart for Aliasing IP Deskphones for switch compatibility on page 25.

Related links

Communication Manager Administration on page 39
Administering features on page 47

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 47

Administering features and CAs for all other IP deskphones

You can administer Feature/Call Appearance Buttons 1 to 24 on the Communication Manager Station form. The features administered on the Station form appear in the same sequence on the deskphone Feature screen.

Features administered on the Expansion Module (SBM24/BM12) Call Appearance buttons display on the deskphone Features screen following the first 24/12 administered feature buttons.

All administered Button Module Labels, Call Appearances and Feature Buttons, display on the corresponding module buttons.

In the Table 1: Station form administration results on page 48 the term *phone screen* refers to either the call appearance screen or the features screen, as applicable to the button type.

Table 5: Station form administration results

Feature / Call Appearance (CA) / Bridged Call Appearance (BA) buttons on the Station form...	Displayed as:			
1 to 3	N/A	9608/9608G/ 9611G	N/A	9621G/ 9641G/ 9641GS
4 to 11	CAs/BAs on Phone screen; must scroll to see more than 3	CAs/BAs on Phone screen: must scroll to see more than 6	Aux buttons 1 to 8 CAs/BAs on Phone screen; must scroll to see more than 3	CAs/BAs on Phone screen; all buttons also appear on the Quick Touch panel (if enabled) and not on the display screen. If Quick Touch panel is disabled, 6 CAs display; switch to Features and scroll to see up to 12 feature buttons
12 to 19	N/A	Scroll to see CAs/ BAs, features on Feature List	Aux buttons 9 to 16	Scroll to see CAs/ BAs, features on Feature List

Table continues…

Feature / Call Appearance (CA) / Bridged Call Appearance (BA) buttons on the Station form...	Displayed as:			
20 to 24	N/A	Features on Feature List	Features on Feature List	Features on Feature List
25 to 48	N/A	1st BM12/SBM24	1st BM12/ SBM24	1st BM12/SBM24
49 to 72	N/A	2nd BM12/SBM24	2nd BM12/ SBM24	2nd BM12/ SBM24
73 to 96	N/A	3rd BM12/SBM24	3rd BM12/ SBM24	3rd BM12/SBM24

For additional information about administering the call server for 9600 Series IP Deskphones, see the following Avaya documents, available on the Avaya Support Web site:

- *Administrator Guide for Avaya Communication Manager*, 03-300509.
- *Feature Description and Implementation for Avaya Communication Manager*, 555-245-770.

Related links

Communication Manager Administration on page 39

Chapter 6: Server Administration

Server Administration

Related links

Software prerequisites on page 50
Administering the DHCP and file servers on page 50
DHCP generic setup on page 51
Setting up the DHCP server on page 52
Setting up a DHCPv6 server on page 58
HTTP generic setup on page 58
Backup and restore processing on page 60
About IPv4 and IPv6 operation on page 62
Features not supporting IPv6 on page 64

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 9600 Series 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 50

Administering the DHCP and file servers

Dynamic Host Configuration Protocol (DHCP) minimizes maintenance for the 9600 Series 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 9600 Series IP Telephones:

- An IP address of the 9600 Series 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 9600 Series IP deskphone can reach a DHCP server that contains the IP addresses and subnet mask.

The 9600 Series IP Deskphone 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 9600 Series IP Deskphone 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 9600 Series IP Deskphone 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. For more information, see Administering options for IP phones on page 70.

Related links

Server Administration on page 50

DHCP generic setup

This document describes the generic DCHPv4 and DHCPv6 administration that works with the 9600 Series 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 50

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 9600 Series IP Deskphones.
   - 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 9600 Series 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 104.
     - **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` parameters:

Code	Parameter
1	Must be the first encapsulated parameter in Option 43 with a value of 6889.

Table continues…

	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	TLSSRVR
6	TLSDIR
7	TLSPORT
9	L2Q
10	L2QVLAN
11	PHY1STAT
12	PHY2STAT
13	PROCSTAT
14	SIG
16	MCIPADD
17	TLSSRVRVERIFYID

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 9600 Series IP Deskphones to restart. Avaya recommends providing enough leases so the IP address of a 9600 Series IP Deskphone 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. For more information, see 9600 Series H.323 customizable system parameters on page 71.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 9600 Series IP Deskphone 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 9600 Series IP Deskphone 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 9600 Series IP Deskphone 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`** =*xxxx.xxx.xxx.xxx*

Result

In the following table, DHCPACK Setting of Parameter Values on page 55 the 9600 Series IP Deskphone sets the following parameter values to the DHCPACK message field and option.

Table 6: 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).
DNSSRVR	Option #6.
HTTPSRVR	The siaddr field, if that field is not a zero.
TLSSRVR	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. For more information, see About Link Layer Discovery Protocol (LLDP) on page 112.

Note:

The 9600 Series IP Deskphones do not support Regular Expression Matching, and therefore, do not use wildcards. For more information, see Administering Options for 9600 Series H.323 deskphones on page 70.

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 50
Configuring DHCP Option 242 on page 55

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 9600 Series IP Deskphones do not support for setting through DHCP in option 242, or
2. Delete unused or unsupported 9600 Series 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 9600 Series IP Deskphones, although most of them can be set in a 46xxsettings.txt file as well.

Table 7: Parameters Set by DHCP in a Site-Specific Option

Parameter	Description
DNSSRVR	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 *SET HTTPDIR myhttpdir*. The path relative to the root of the TLS or HTTP file server where 9600 Series 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 46xxsettings.txt 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 to download the HTTP file.
HTTPSRVR	Specifies the IP addresses or DNS names of HTTP file servers used to download 9600 Series 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 46xxsettings.txt 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.
PHY1STAT	Controls the Ethernet line interface speed. The default is 1 which indicates that it is auto-negotiate.

Table continues…

Parameter	Description
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 n umber 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 46xxsettings.txt 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 a settings 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 HTTPS file downloading.
TLSSRVR	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 9600 Series 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 52

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 documented in the section Features not supporting IPv6 on page 64. 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 DNSSRVR 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 50

HTTP generic setup

About this task

You can store the same application software, script file, and settings file on an HTTP server. The 9600 Series IP Deskphone uses the application software, script file, and settings file. The 9600 Series IP Deskphone might lose some functionality, if you reset the HTTP server or the HTTP server is unavailable. MVIPTEL and IIS6 are not supported with HTTPS. When using HTTPS, before upgrading, you must replace the server. For more information, see Administering the DHCP and File Servers on page 50.

Caution:

Ensure that the files defined by the HTTP server configuration are accessible from all 9600 Series 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 65.

   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:

   9600 Series IP Deskphones H.323 v6.6.2 and later do not support HTTPS with MV_IPTEL 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 TLSSRVR to the addresses of the Avaya HTTPS server.

Related links

Server Administration on page 50
HTTP Redirect feature on page 60

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 TLSSRVR) for different groups of phones.

You do not 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 58

Backup and restore processing

9600 Series 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:

9600 Series IP Deskphones H.323 v6.6.2 and later do not support HTTPS with MV_IPTEL 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.

For deletion, the initiating process must only supply the file name. The server requests deletion of the file through an HTTP DELETE message. The initiating process receives a success indication, if a 2xx HTTP status code is received, 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 downloaded 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 9600 Series IP Deskphones or the Prompt Line for all other 9600 Series IP Deskphones display an HTTP Authentication or an HTTP Authentication Failure interrupt screen: `Enter backup/restore 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.

For specific error messages relating to backup or restore, see the *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694*.

Related links

Server Administration on page 50

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 with known limitations documented in the section Features not

supporting IPv6 on page 64. 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 8: IP Enablement Results

Manually programmed 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 50

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 9: 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 50

Chapter 7: Telephone software and application files

Telephone Software and Application Files

Related links

[Understanding the general download process](#) on page 65
[Using the GROUP parameter to set up customized groups](#) on page 68

Understanding the general download process

9600 Series IP Deskphones download upgrade files, settings files, language files, certificate files, and software files from a file server. 9600 Series 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 9600 Series 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.

9600 Series IP Deskphones H.323 v6.6.2 and later do not support HTTPS with MV_IPTEL 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, 9600 Series IP deskphones might not contain the latest software. When you first plug in the 9600 Series 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
- IIS6
- IIS7.5
- IIS8
- Utility Server

Important:

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

The 9600 Series IP deskphones then downloads a 46xxsettings.txt file. The settings file contains options that you have administered for any or all the phones in your network. For more information about the settings file, see About the settings file on page 67. After downloading the settings 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 65
Choosing the right application file and upgrade script file on page 66
Using the upgrade file on page 67
About the settings file on page 67

Choosing the right application file and upgrade script file

Software files needed to operate the 9600 Series IP Deskphones 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.

For detailed information about downloading files and upgrading telephone software, see *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694* 16-300694 for all releases less than 6.0. For Release 6.1 and later covering the 9608, 9611G, 9621G, and 9641G deskphones, see *Installing and Maintaining Avaya 9608/9608G/ 9611G/9621G/9641G/9641GS IP Deskphones H.323*, 16-603603.

Related links

Understanding the general download process on page 65

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 settings file name, if desired, as long as you also edit the corresponding **GET** command in the upgrade script file.

Related links

Understanding the general download process on page 65

About the settings file

The settings file contains the option settings you need to customize the Avaya 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.

For more information on parameters and valid values, see 9600 Series H.323 customizable system parameters on page 71.

Related links

Understanding the general download process on page 65

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 a 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. See *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694*. 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 65

Chapter 8: Administering Deskphone Options

Administering Deskphone Options

Administering options for 9600 Series H.323 Deskphones

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 9600 Series 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.

For more information on craft options, see the *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694*.

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:

For information on the system parameters related to Virtual Private Network (VPN) setup and maintenance, see *VPN Setup Guide for 9600 Series IP Telephones*, 16-602968.

The following table lists the parameters that are described in that document:

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.

9600 Series 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
ADMIN_HSEQUAL	1	Handset Equalization alternative permission flag. Valid values are: 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. **Note:** 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.
AGCHAND	1	Automatic Gain Control status for handset, 0=disabled, 1=enabled. **Note:** 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.
AGCHEAD	1	Automatic Gain Control status for headset, 0=disabled, 1=enabled. **Note:** 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.
AGCSPKR	1	Automatic Gain Control status for Speaker, 0=disabled, 1=enabled. **Note:** 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/

Table continues…

Parameter name	Default value	Description and value range
		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.
AGENTGREETINGSDELAY	700	Valid values: 0 – 3000 where the value specifies the delay time (milli seconds) between call autoanswer and playing of an agent greeting.
AGTACTIVESK	0	Used to control the softkeys that are available to the agent on the deskphone. If value = 0, Transfer softkey is available on the second row of softkeys, and Release on the first row. If value = 1, Release softkey is available on second row of softkeys, and Transfer on the first row. If value = 2, Release softkey is not available on first/ second row of softkeys, because there can be more softkeys with value 2 other than mentioned. If value =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	For Avaya Call Center use only. 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. 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. 1 ASCII numeric digit. Valid values are: 1 = Invoke the caller information permission to locate a greeting. 0 = Do not automatically invoke Call-info permission.
AGTCAINFOLINE	1	Controls presentation of call associated information in the agent information line when the phone is in half width screen mode. Valid values are: • 0: The Agent Information Line presents agent-oriented information only.

Table continues…

Parameter name	Default value	Description and value range
		• 1: The Agent Information Line presents agent-oriented information and call associated information.
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: 1 = Disable the Forward button. 0 = Do not 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: 1 = Display the Greeting softkey upon alerting. 0 = Do not 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 (#)
AGTSPKRSTAT	1	For Avaya Call Center use only. Disables or enables the speakerphone permission flag. 1 ASCII numeric digit. Valid values are: 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

Table continues…

Parameter name	Default value	Description and value range
		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. 4=
AGTTIMESTAT	1	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: 1 = Do not display date and time on the top display line. 0 = Display the date and time on the top display line.
AGTTRANSLTO	to	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. Tthe Agent Information line displays the result and provides information about the incoming call. 1 to 6 UTF-8 characters.
AGTTRANSCLBK	callback	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.
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

Table continues…

Parameter name	Default value	Description and value range
		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: 1=all applications enabled, 2=Speed Dial (Contacts) changes and Call Log disabled and Redial last number only, 3=Speed Dial (Contacts) changes disabled, 0=Speed Dial (Contacts) changes, Call Log, and Redial disabled.
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: • 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:

Table continues…

Parameter name	Default value	Description and value range
		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 *Audio Quality Tuning for IP Telephones*,100054528 on the Avaya Support site at www.avaya.com/support.
AUDIOSTHS	0	Handset sidetone setting. Valid values are: 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 *Audio Quality Tuning for IP Telephones*, 100054528 on the Avaya Support site at www.avaya.com/support.
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).

Table continues…

Parameter name	Default value	Description and value range
BLUETOOTHSTAT	1	Bluetooth permission flag. 0=Bluetooth is disabled, 1= Bluetooth is enabled. When Bluetooth is disabled through BLUETOOTHSTAT, the user cannot override this setting locally on the deskphone.
BRAUTH	0	Backup/restore authentication control. Valid values are: 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. 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.
BRURI	“ ” (Null)	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. 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. For example: SET BRURI http://Administrator:Catt*123@10.10.10.6/Backup/ SET BRURI http://ipphone:Avaya1234@10.10.10.1
CADISPMODE	0	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: • 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

Table continues…

Parameter name	Default value	Description and value range
		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	Applies only to deskphones running software Release 6.0 and later. Specifies whether the Calculator application must be displayed or enabled. Valid values are: 1=Yes, enable the Calculator application, 0=No, disable the Calculator application.
CALLCTRSTAT	0	Applicable only to Call Centers. Call Center functionality flag. 1 ASCII numeric digit. Valid values are: 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. **Note:** This parameter is soft persistent.
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: • 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

Table continues…

Parameter name	Default value	Description and value range
		CLBACKUPTIME. This parameter only has an effect if the value of LOGBACKUP is 1. Valid values are: • 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: • 0: The deskphone uses the values of these parameters. • 1: The deskphone ignores the values those parameters.
CCLOGOUTIDLESTAT	0	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: =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. **Note:** 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.
CLDELCALLBK	0	Call Log Delete Callback Flag. Deletes calls from the Missed Call Log when the user returns the call from the Call Log. Values are 1=No, 0=Yes.
CLDISPCONTENT	1	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: • 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.

Table continues…

Parameter name	Default value	Description and value range
CLEAR_EXTPSWD_ON_LOGOUT	0	Specifies whether the extension and password are not displayed on a logged out deskphone. Valid values are: • 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	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. Valid values are 0 to 99. The value 0 disables the warning.
CONFSTAT	0	Specifies whether the conference button is enabled or disabled when CCBTNSTAT is 0. Valid values are: • 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. • 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: 4=DHCPv4 is preferred. 6= DHCPv6 is preferred.

Table continues…

Parameter name	Default value	Description and value range
DHCPSRVR	“ ” (Null)	Specifies DHCP server address(es). Format is dotted decimal or DNS format, separated by commas, with no spaces. Zero to 255 ACSII 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 1, (No) the deskphone strictly follows the DHCP standard with respect to giving up IP addresses when the DHCP lease expires. If set to 0,(Yes) the deskphone continues using the IP address until it detects reset or a conflict.
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 zero to five whole numbers separated by commas without any spaces.
DNSSRVR	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: 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 *MD5* and *TLS* .
DOT1XSTAT	0	Determines how the deskphone handles Supplicants. Valid values are: 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 telephone will wait for 802.1X authentication to complete before initiating DHCP Valid values, 0 and 1 If DOT1XWAIT = "0" when the 802.1X Supplicant is started, startup will continue without waiting for 802.1X authentication to complete, =1 Startup will not continue.,
DROPCLEAR	1	VPN only. Specifies how clear IPsec packets are processed. One ASCII numeric digit. Valid values are: 0=

Table continues…

Parameter name	Default value	Description and value range
		all other packets will be processed, but not by IPsec, or 1=all other packets will be discarded.
DROPSTAT	0	Specifies whether the Drop button is enabled or disabled when CCBTNSTAT is 0. Valid values are: • 0: The Drop button is disabled when CCBTNSTAT is 0. • 1: The Drop button is enabled.
ENHDIALSTAT	1	Specifies the dialing algorithm status. Controls whether algorithm defined by parameters is used during certain dialing behaviors. Valid values are: • 0: Disables algorithm. • 1: Enables algorithm, but not for Contacts. • 2: Enables algorithm, including Contacts. If set to 1, the Administering dialing methods feature is on for all associated applications.
FBONCASCREEN	0	Specifies whether the Feature buttons are displayed on the same screen as Call Appearance when the value of PHNSCRALL is 0. Applies only to 9608, 9608G, and 9611G deskphones. • 0: Deskphone does not display Feature buttons on the Call Appearance screen. • 1: Deskphone displays Feature buttons that can adjust on the Call Appearance screen. In addition, the deskphone has a separate screen for Features.
FIPS_ENABLED	0	Allows only FIPS 140-2 Level 1 validated cryptographic algorithms. To enable the JITC mode, set the value to 1.
GRATARP	0	Gratuitous ARP flag. Controls whether the deskphone processes gratuitous ARPS or ignores them. 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. Valid values are: 1 = Yes, process gratuitous ARPS 0 = No, ignore gratuitous ARPS
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

Table continues…

Parameter name	Default value	Description and value range
		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 *GUESTLOGINDURATION* 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: 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 gnored by the deskphones that do not have a Headset button. Valid values are: • 0: The Headset button is disabled when CCBTNSTAT is 0. • 1: The Headset button is enabled.
HEADSETBIDIR	0	Specifies the permission flag for enabling or disabling the Headset Bi-directional functionality. Valid values are: 0= Default, Bi-directional functionality disabled, 1= Switchhook and Alerting, 2= Switchhook only. **Note:** 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.
HOLDSTAT	0	Specifies whether the Hold button is enabled or disabled when CCBTNSTAT is 0. Valid values are: • 0: The Hold button is disabled when CCBTNSTAT is 0.

Table continues…

Parameter name	Default value	Description and value range
		• 1: The Hold button is enabled.
HOMEIDLETIME	10	For touchscreen deskphones only, the number of minutes after which the Home screen will be displayed. Value is 1 or 2 ASCII numeric digits, 0 through 30. If you prefer an idle Web page as the display instead of the Home screen, set this value to less than the WMLIDLETIME value.
HOOKSTAT	0	Specifies whether the switchhook is enabled or disabled when CCBTNSTAT is 0. Valid values are: • 0: The switchhook is disabled when CCBTNSTAT is 0. • 1: The switchhook is enabled.
HTTPDIR	“ ” (Null)	HTTP server directory path. The path name prepended to all file names used in HTTP *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 *SET HTTPDIR myhttpdir*” where *myhttpdir* 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. • 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: 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

Table continues…

Parameter name	Default value	Description and value range
		six whole numbers separated by commas without any intervening spaces. **Note:** 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.
IPPREF	6	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: 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	Applies only to deskphones running software Release 6.0 and later. Specifies whether IPv6 will be enabled. Valid values are: 0 = IPv6 is disabled. 1 = IPv6 is supported/ enabled. **Note:** 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.
L2Q	0	Controls whether Layer 2 frames have IEEE 802.1Q tags (0=auto, 1=enabled, 2=disabled).
L2QVLAN	0	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. 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.
LANG0STAT	1	Controls whether the built-in English language text strings can be selected by the user. Valid values are: 0 = User cannot select English language text strings 1 = User can select English language text strings. SET LANG0STAT 1

Table continues…

Parameter name	Default value	Description and value range
LANGxFILE	“ ” (Null)	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`” LANG1FILE = LANG2FILE = LANG3FILE = LANG4FILE =
LANGLARGEFONT	“ ” (Null)	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.
LANGSYS	“ ” (Null)	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` **Note:** 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.
LEDMODE	0	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 . Example: If new behavior is activated, Button module and phone LEDs are aligned and will change according to call state.
LLDP_XMIT_SECS	30	Specifies the rate in seconds at which LLDP messages will be transmitted. Valid values are 1 to 4 ASCII numeric digits, “1” through “3600” Main usage is for the SSO application to discover the phone faster.
LOCALZIPTONEATT	35	Controls the local phone ziptone volume when AUTOANSSTAT= 1 Note: If Auto answer is configured on

Table continues…

Parameter name	Default value	Description and value range
		the CM and not using the AUTOANSSTAT setting, this parameter does not influence that zip tone volume. Valid values: 0-95 where 0= Loudest and 95= Lowest.
LOGBACKUP	1	Indicates whether the call log of the user should be backed up. Values are: 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. 0=No.
LOGLOCAL	0	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: 0=Disabled, 1=emergencies, 2=alerts, 3=critical, 4=errors, 5=warnings, 6=notices, 7=information, 8=debug.
LOGMISSEDONCE	0	Indicates that only one Call Log entry for multiple Missed calls from the same originating phone number must be maintained. Values are: 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. 0=No; each Missed Call creates a new Call Log entry.
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	Indicates that a Call Log entry should be maintained for calls that are redirected from the deskphone, for example, Call forwarded calls. Values are: 1=Yes; 0=No. CM 5.2 or later is required for this feature to work.
LOGTOFILE	0	Specifies whether optional debug printf strings will be logged to an internal file. If LOGTOFILE=1, optional debug printf strings are logged to an internal file, =0 not logged.
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

Table continues…

Parameter name	Default value	Description and value range
		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: • 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".
MYCERTRENEW	90	Percentage of a certificate's Validity interval after which renewal procedures will be initiated. 1 or 2 ASCII numeric digits, 1 through 99.
MYCERTURL	“ ” (Null)	URL to be used to contact an SCEP server. Zero to 255 ASCII characters, zero or one URL.
MYCERTWAIT	1	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: 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. 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.

Table continues…

Parameter name	Default value	Description and value range
NDREDV6	0	Applies only to deskphones running software Release 6.0 and later. Controls whether IPv6 Neighbor Discovery Redirect messages will be processed. Valid values are: 0= Ignore received Redirect messages. 1= Process received Redirect messages.
NVHTTPSRVR	“ ” (Null)	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. 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 *VPN Setup Guide for 9600 Series IP Telephones*,16-602968.
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.
NVTLSSRVR	“ ” (Null)	VPN and non-VPN. HTTPS file server IP addresses used to initialize TLSSRVR 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 *VPN Setup Guide for 9600 Series IP Telephones* ,16-602968.
OCSP_ACCEPT_UNK	1	Specifies whether a certificate is authenticated even if its revocation status cannot be determined. Valid values are: • 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: • 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.

Table continues…

Parameter name	Default value	Description and value range
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: • 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.
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 *abc*, where each letter represents a 0 (disabled/off) or 1 (enabled/on), interpreted as: *a* = base settings for all user options and related applications, except as in *b* or *c*. *b* = setting for view-oriented applications (for example, the Network Information application), as applicable. *c* = 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.

Table continues…

Parameter name	Default value	Description and value range
		Note that the value of CALLCTRSTAT must be 1 for OPSTATCC to be used. 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.
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: • 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

Table continues…

Parameter name	Default value	Description and value range
		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. • 0: Separate screens for Call Appearance and Feature buttons. • 1: Consolidated screen for Call Appearance and Feature buttons.
PHNSCRCOLUMNS	0	Valid values are 0 or 1 Specifies whether the Phone Screen is presented with one (full-width) or two (each half-width) columns. **Note:** 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. • 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. The CLEAR operation clears the user configuration.
PHY1STAT	1	Ethernet line interface setting 1=auto-negotiate, 2=10 Mbps half-duplex, 3=10 Mbps full-duplex, 4=100 Mbps half-duplex, 5=100 Mbps full-duplex, and 6=1000 Mbps full-duplex, if supported by the hardware.
PHY2PRIO	0	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.
PHY2STAT	1	Secondary Ethernet interface setting, 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), and 6=1000 Mbps full-duplex if supported by the hardware.

Table continues…

Parameter name	Default value	Description and value range
PHY2VLAN	0	VLAN identifier used by frames received on or forwarded to the secondary Ethernet interface. Set this parameter only when VLAN separation is “1” (enabled). 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.
PKCS12URL	NULL	Specifies the URL to download a PKCS #12 file containing an identity certificate and its private key. Value is a string that contains either of the following variables, along with other characters: • `$SERIALNO`: Is replaced by the serial number of the deskphone. • `$MACADDR`: Is replaced by the MAC address of the deskphone. Must be specified without colons. For example, For example, if Ethernet MAC address of a specific phone is `00-24-D7-E4-2E-98` and the PKCS12URL is `http://pkc12file_$MACADDR.cer`, then the filename of the PKCS12 file for this phone on the file server will be `pkc12file_0024D7E42E98.cer`.
PINGREPLYV6	1	Specifies whether ICMPv6 Echo Reply messages will be sent or not. Valid values are: 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.
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).

Table continues…

Parameter name	Default value	Description and value range
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: 1= Quick login permitted; user must press the pound (#) key to see the previous Extension and Password. 0= Quick login not permitted; the user must explicitly enter the 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. (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_INTERVAL	15	Recording tone interval. The number of seconds between recording tones, with a range from 1 to 60.
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

Table continues…

Parameter name	Default value	Description and value range
		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 , 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.
SCREENSAVER	“ ” (Null)	Filename for a custom screen saver. 0 to 32 ASCII characters. Note that screen saver files must be in .jpg format. Acceptable characters for use in filenames are: 0 through 9 A through Z a through z - (dash) . (period) _ (underscore)
SCREENSAVERON	240	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.
SERVER_CERT_RECHECK_HOURS	24	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. Valid values are 0 to 32767. The value 0 stops the verification.
SLMCAP	0	Specifies whether the SLA Monitor agent supports packet capture. Assign one of the following values. • 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.

Table continues…

Parameter name	Default value	Description and value range
SLMCTRL	0	Specifies whether the SLA Monitor agent supports device control. Assign one of the following values. • 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	Valid values are 0 or 1 Specifies whether the SLA Monitor agent supports performance monitoring.
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	Valid values, any 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.

Table continues…

Parameter name	Default value	Description and value range
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: 0= Default , SSO disabled. 1=SSO enabled.
SSO_CLIENT_CERT	0	Specifies whether the telephone will request and authenticate an identity certificate from the desktop computer during the TLS handshake for SSO. Valid values are: 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	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: 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. **Note:** If the SSO TCP connection is terminated but the link is not lost, no action is taken based on this parameter.
SSO_DISCONNECT_FACS	“null string”	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	Specifies what the telephone does if the telephone receives a Lock or Unlock command from the SSO application. Valid values are: 1= Default, the telephone attempts to run the LOCK command. 0 = the telephone ignores the LOCK command.

Table continues…

Parameter name	Default value	Description and value range
SSO_REGISTERED_MODE	1	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. 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	Signaling protocol download flag. Valid values are: 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. 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.
SYSAUDIOPATH	0	For Avaya Call Center use only 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: 0 = Default value. The agent can select the audio path through option & 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. **Note:** By implication, if the 46xx settings file contains a non-default value for SYSAUDIOPATH, the setting for SYSAUDIOPATH overrides any user-specified settings for the audio path.

Table continues…

Parameter name	Default value	Description and value range
TIMERSTAT	0	TIMERSTAT specifies whether Timer On and Timer Off softkeys will be presented to the user. 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)	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 *SET TLSDIR mytlsdir* where *mytlsdir* is your HTTPS server path. TLSDIR is the path for all HTTPS operations except for BRURI.
TLSPORT	80	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 81 which is the port required for HTTPS downloads rather than the using the default.
TLS_SECURE_RENEG	0	Specifies whether a TLS session should be terminated if the peer does not support secure renegotiation. Valid values are: • 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: • 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).

Table continues…

Parameter name	Default value	Description and value range
TLS_VERSION	0	Controls the TLS version that is used for all TLS connections. Valid values are: • 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: • 0: Tags not allowed in the VPN mode. • 1: Tags allowed in the VPN mode.
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
WBCSTAT	1	Valid values are 1 to 6 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: • 0: The Transfer button is disabled when CCBTNSTAT is 0. • 1: The Transfer button is enabled.

Note:

The preceding table applies to all 9600 Series IP deskphones. Certain 9600 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 9600 Series IP deskphones 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 102
The VLAN default value and priority tagging on page 103
Automatic detection of a VLAN on page 103

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 9600 Series 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 9600 Series 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 102

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 9600 Series IP Deskphone 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 102

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 9600 Series 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.

For more information on the Reset procedure, see *Installing and Maintaining Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323*.

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 102

About DNS addressing

The 9600 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 DNSSRVR and DOMAIN values so that you can use those names later in the script.

Note:

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

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 105
Activating EAP-TLS for authentication on page 106
Scenarios for using EAP-TLS based authentication on page 107
Deploying EAP-TLS based authentication for phones using 802.1x and MD5 on page 107
Deploying EAP-TLS on phones running without any type of 802.1x authentication on page 109

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 9600 Series 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 105

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 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 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 105

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 105

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 105

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 105

About IEEE 802.1X

9600 Series 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 9600 Series 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 111

802.1X supplicant operation

9600 Series IP Deskphones 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 110

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 9600 Series IP deskphones 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 9600 Series IP deskphone 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 10: 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.

Table continues…

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

Table continues…

Category	TLV Name (Type)	TLV Info String (Value)
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 11: Impact of TLVs Received by 9600 Series IP deskphones on 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.
L2QVLAN and L2Q	IEEE 802.1 VLAN Name	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: • 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. 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. 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 *on* changes the default L2Q to *on* and resets. If there is no valid IP Address, the phone immediately starts tagging with the new VLAN ID without resetting.
L2Q, L2QVLAN, L2QAUD, L2QSIG, DSCPAUD, DSCPSIG	MED Network Policy TLV	L2Q - set to 2 (off) If T (the Tagged Flag) is set to 0; set to 1 (on) if T is set to 1. L2QVLAN - set to the VLAN ID in the TLV. L2QAUD and L2QSIG - set to the Layer 2 Priority value in the TLV. DSCPAUD and DSCPSIG - set to the DSCP value in the TLV.

Table continues…

System Parameter Name	TLV Name	Impact
		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: • 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.
L2Q	Proprietary 802.1 Q Framing	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. • 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. But, the 9670G deskphone puts the display backlight into low-power mode and does not turn off the backlight.
	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

Installing and Maintaining Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323 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 and any non-color deskphones.
- DEBUG - Enable or disable debug mode for the button module serial port.
- 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 - 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 - 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 the 9600 IP deskphone 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, 9600 Series IP deskphones display 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.

For touch screen deskphones, this information includes an indication of the character that you can use as a decimal in numeric values and an indication of the character that you should use as a separator. For example, thousands or millions in numeric values. You cannot use a character or a space character as punctuation marks.

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	

Administering dialing methods

9600 Series IP deskphones have 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 12: 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	WMLHOME. **Note:** If WMLHOME is null, the deskphone screen displays *WML Applications Help icon* by default, You can suppress the display by setting WMLHELPSTAT to 0.	You administer the WML applications in the AvayaMenuAdmin.txt file. 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. If WMLHOME is null and the value of WMLHELPSTAT is not 1, the deskphone does not display any WML items .

Table continues…

Application	Parameter and value	Dependency
World Clock application	WORLDCLOCKAPP	The **WORLD CLOCK** application displays unless WORLDCLOCKAPP is null.
Weather application	WEATHERAPP	The **Weather** application displays sunless WEATHERAPP is null.
My Pictures	SCREENSAVERON	**My Pictures** displays if and only if SCREENSAVERON is non-null.
Calculator	CALCSTAT	The **deskphone displays the Calculator** application unless CALCSTAT is 0.
Settings application	N/A	The **Settings** application always displays unless suppressed by OPSTAT.
Greetings	N/A	The **Greetings** program displays only if you configure the following conditions: • 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. **Note:** The agent greetings can be recorded and played only by using the headset or the speaker.
User defined contact favorites	N/A	The user can display up to 16 favorites. If the user has set only one contact as favorite, then an item labeled Favorites Help displays after Contacts Favorite. Favorites Help is unavailable if a temporary contacts list from a USB flash drive is in use.

Table continues…

Application	Parameter and value	Dependency
		Note: If the system suppresses the backups when BRURI is null, then the user loses the Favorites and all other Contacts when the user logs out. If the administrator has set APPSTAT to a value other than 1, the user cannot make changes to Contacts, so the administrator might prepopulate Contacts, and enable or disable entries to display the contacts as Favorites or not.

Related links

WML browser properties on page 121

WML browser properties

The following table shows a comparison of the WML browser properties of the deskphones:

Feature	9608/9608G	9611G	9621G	9641G
Top line	Yes	Yes	Yes	Yes
Application lines	4	4	4	5
Line buttons	Yes	Yes	No	No
Selectable objects per line	1	1	1	1
Application line height (in pixels)	15	31	38	38
Softkeys per screen	4	4	5	5
Navigation buttons	Yes	Yes	No	No
Text input	Yes	Yes	Yes	Yes
Color support	No	Yes	Yes	Yes
Supported image format	JPEG	JPEG	JPEG	JPEG
Maximum image width (in pixels)	175	300	430	430
Maximum image height (in pixels)	1440	2976	3648	3168
Click to dial	Yes	Yes	Yes	Yes

Table continues…

Add to phonebook	Yes	Yes	Yes	Yes
Characters per line (normal font)	31	40	39	39
Characters per line (large font)	25	22	26	26
Characters per softkey (normal font)	8	8	8	8
Characters per softkey (large font)	6	6	8	8

Related links

Managing applications on the Home screen on page 119

Administering features on softkeys

You can administer call server features on softkeys on the deskphhone. The number of features you can place on a set of softkeys depends on the call state the deskphone 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

Note:

For more information about the system parameters, see 9600 Series H.323 customizable system parameters on page 71.

Administration of softkeys works as follows:

- Administer feature buttons for the deskphone on the call server as you normally would, and the call server sends these button assignments to the deskphone as it always has.
- In the 46xxsettings 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. CM Feature Numbers for Assigning Softkeys on page 124 lists the administrable features and their associated numbers.

- The deskphone 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 deskphone 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 numbers listed in CM Feature Numbers for Assigning Softkeys on page 124, 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 deskphone. This means the corresponding softkey is labeled Redial if the deskphone 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 deskphone 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 any SBM24 button module are ignored. The feature must be administered for the deskphone 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 deskphone 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 deskphone. For example, using the IDLEFEATURES, you can specify up to six features, although any one deskphone 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 deskphones. Since the deskphone 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 deskphones will set the alert to a single short ring followed by visual ringing alerts only.

The Feature Numbers are as follows.

Table 13: CM Feature Numbers for Assigning Softkeys

Feature Name	Default Label	Feature Number
abr-prog	AbbrvDial Program	67
abr-spchar	AbrvDial (char)	68
abrv-dial	AD	65
abrv-ring	AR	226
ac-alarm	AC Alarm	128
aca-halt	Auto-Ckt Assure	77
account	Acct	134

Table continues…

Feature Name	Default Label	Feature Number
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-requst	ANI Request	146
assist	Assist	90
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-alrm	CDR 1 Failure	106
cdr2-alrm	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

Table continues…

Feature Name	Default Label	Feature Number
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
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

Table continues…

Feature Name	Default Label	Feature Number
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
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-alrm	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-alrm	Maj/Min Hdwe Failure	82
mm-basic	MM Basic	169
mm-call	MM Call	167
mm-cfwd	MM CallFwd	244

Table continues…

Feature Name	Default Label	Feature Number
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
next	Next	13
night-serv	Night Serv	53
noans-alrt	RONA	192
no-hld-cnf	No Hold Conference	337
normal	Nornal 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

Table continues…

Feature Name	Default Label	Feature Number
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
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
togle-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 9600 Series IP deskphones 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 9600 Series 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.

- **Local Procedure**: When users are denied access to Options for administrative reasons, but individual users need an equalization value other than the one in the settings file, the HSEQUAL Local Procedure as documented in the *Installing and Maintaining Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323* for 9608, 9611G, 9621G, and 9641G deskphones provides another method to administer the deskphone with the audio equalization value that you require. “Default” uses the settings file value unless superseded by User Option. “Audio Opt.” is optimized for TIA-810/920 acoustic performance, and “HAC Opt.” is optimized for HAC telecoil performance.
- **User Option**: The user can select “Default” by which the deskphone uses the settings file value unless superseded by Local Procedure), “Audio Opt.” which uses Handset equalization that is optimized for acoustic TIA 810/920 performance, or “HAC Opt.” which uses Handset equalization that is optimized for electrical FCC Part 68 HAC telecoil performance.
- Handset equalization options are effected in the following order:
  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** and **HAC Opt** that are available for Handset equalization are mutually exclusive, meaning only one can be activated at a time.

Administering deskphones for call center operation

The 9608, 9608G, 9611G, 9621G, 9641G, and 9641GS H.323 deskphone models can be used in call centers. These deskphones use the call center features provided by Avaya Aura® Communication Manager.

Use the 46xxsettings file to customize the deskphone parameters associated with call center operations. These parameters allow the agents to access different functions, such as:

- AGTCALLINFOSTAT - Provides agent access to automatic caller information.
- AGTFWDBTNSTAT - Prevents agents from forwarding calls while signed in.
- AGTGREETINGSTAT - Gives an agent permission to record or select a greeting.
- AGTLOGINFAC - Indicates which Feature Access Code agents must dial to sign in to the call center.
- AGTSPKRSTAT - Allows or disallows agents from disabling the speakerphone.
- AGTTIMESTAT - Displays the time and date on the top display line.
- AGTTRANSLTO -Determines the proper Agent Information message regarding an incoming call.

- AGTTRANSCLBK - Determines the proper Agent Information message regarding an incoming call.
- AGTTRANSLPRI - Determines the proper Agent Information message regarding an incoming call.
- AGTTRANSLPK - Determines the proper Agent Information message regarding an incoming call.
- AGTTRANSLICOM - Determines the proper Agent Information message regarding an incoming call.
- CALLCTRSTAT - Provides agent access to call center features for the phone, including Greetings.
- OPSTATCC - Overrides the OPSTAT parameter setting to allow agent access to related Options & Settings. It 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

You must configure the following Communication Manager call center buttons on the deskphone:

- Auto-In
- Manual-In
- After Call Work (ACW)
- Aux Work

Important:

Communication Manager can be set to send the user to the ACW mode after a call ends. You must configure the ACW button on the deskphone to prevent the agent being logged out at the end of each call.

For more information about these parameters, see 9600 Series H.323 customizable system parameters on page 71.

For additional information on agent and call centers, see *Using Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323 for Call Center Agents*, 16-603613.

Ringing on wireless headset

Ringing on wireless headsets from Jabra and Plantronics can be configured by the administrator and is supported as of Release H.323 6.2 Service Pack 2. Using this feature, you can enable ringing on the wireless headset in addition to the speaker. The ringing tone on the speaker may be turned off using the AUDASYS parameter.

Note:

By default, this feature is set to 0 and is disabled. For deskphones that are used without wireless headset with the bidirectional interface support this feature must be turned off.

To enable this feature, SET HEADSETBIDIR=1 in the 46xxsettings file.

When the base unit is powered on, either one of the following scenarios might occur:

- When the user goes off-hook with the headset or change from a non-headset device to the headset, the wireless headset is activated.
- When the user goes on-hook on the deskphone with an activated headset or change from wireless headset device to non-headset, the wireless headset is deactivated.

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 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 14: 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 value	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

Table continues…

		logged into a call center (regardless of status such as Ready, Aux Work, etc.)
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

9600 Series IP Deskphones support 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:

9600 Series IP Deskphones H.323 v6.6.2 and later do not support HTTPS with MV_IPTEL 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

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.

For specific error messages relating to Backup/Restore, see the *Avaya IP Deskphone Edition for 9600 Series IP Telephones, Installation and Maintenance Guide, 16-300694*.

Related links

Backup file formats on page 137
User data saved during backup on page 138
About restore on page 140

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 15: Backup File Formats

Item/Data Value	Format
Generic	*name=value*
Contacts	ABKNAME*mmm*=ENTRY_NAME ABKNUMBER*mmm*=ENTRY_NUMBER_1 ABKTYPE*mmm*=ENTRYT_TYPE (where *mmm* is the one-, two-, or three-digit entry ID, with leading zeros for single and double-digit entry IDs)
Call Log entries	CLNAME*mmm*=ENTRY_NAME CLNUMBER*mmm*=ENTRY_NUMBER CLTYPE*mmm*=ENTRY_TYPE CLDATE*mmm*=ENTRY_DATE CLTIME*mmm*=ENTRY_TIME CLDURATION*mmm*=ENTRY_DURATION CLBRIDGEDFLAG*mmm*=ENTRY_BRIDGEDFLAG CLMISSEDCNTR*mmm*=ENTRY_COUNTER CLBCALBL*mmm*=ENTRY_BCALBL

Table continues…

Item/Data Value	Format
	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.
User-generated Call Appearance labels with button identifiers of *mm* where *mm* is the one- or two-digit button number of the entry with a lead zero for single-digit numbers.	PHNLABEL*mm*=CAUSERLABEL
User-generated deskphone Feature Button labels with button identifiers of *mm*, where *mm* is the one- or two-digit button number of the entry with a lead zero for single-digit numbers.	PHNLABEL*mm*=FBUSERLABEL
User-generated SBM24 Call Appearance or Feature Button labels with button identifiers of *mm*, where *mm* is the one- or two-digit button number of the entry with a lead zero for single-digit numbers.	SBMLABEL*mm*=CAUSERLABEL or FBUSERLABEL, as applicable

Related links

Administering backup and restore on page 135

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 16: Options and non-password parameters saved during backup

Parameter Name	Setting
HOMEFAV*nn*	Contact Favorites data. Applicable to touchscreen phones only. An entry is backed up for each Home screen favorite, where *nn* is the index number for that favorite. The backup file format for a Favorite is: HOMEFAV*nn*=*Fav_Number*<US>*Fav_Caption*<US>*Contact_Name* where Fav_Number is the phone number associated with the Favorite, Fav_Caption is the Favorite's caption text, Contact_Name is the Name for the associated Contact entry, and <US> is the Unit Separator (0x001F Unicode value). Upon Restore, a link must be established between a Favorite and a Contact entry by matching the Contact_Name against a Contact's Name and Fav_Number against one of that Contact's numbers. If no match is found, then the Favorite cannot be restored and is discarded.

Table continues…

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
OPTHOMEIDLE	Home Screen on idle; 9621G/9641G/9670G only
OPTTEXTSIZE	Text Size
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
PHNQUICKPANEL	Quick Touch Panel; 9621G/9641G/9670G only
PHNREDIAL	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

Table continues…

Parameter Name	Setting
WEATHERLOCID	Weather Location ID; 9621G/9641G/9670G only
WEATHERUNITS	English/Metric; 9621G/9641G/ 9670G only
WORLDCLOCKLIST	List of World Clock location entries; 9621G/9641G/ 9670G only

Related links

Administering backup and restore on page 135

About restore

When automatic or user-requested retrieval of backup data is initiated, user data and option settings are set to 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 options 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*. For specific formats, see Backup file formats on page 137.
- 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 button labels for an SBM24 button module unit 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 135

Chapter 9: Administering Applications and Options

Administering Applications and Options

Related links

Customizing Applications and Options on page 142
Setting the Application Status flag on page 143
Administering the Avaya A Menu on page 145
Special Administration for Touchscreen Deskphones on page 146
Administering WML applications on the Avaya Menu on page 146
Administering the Avaya Menu with WML applications on page 147
How the Home screen displays WML applications on page 149
Sample Avaya Menu Administration File Template on page 152
Administering guest users on page 154
Administering visiting users on page 154
Idle timer configuration on page 155

Customizing Applications and Options

9600 Series IP deskphones have 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 deskphones needs key information about the servers providing those facilities. You must provide the information in the 46xxsettings.txt file, depending on the applications you want to make available to your end users.

Caution:

For the deskphones to work properly, you must have a *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 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

Calculator application parameter - CALCSTAT

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 - FBONCASCREEN

User Timer (Stopwatch) — TIMERSTAT

VPN parameters - VPN parameters. For more information on VPN parameters, see *VPN Setup Guide for 9600 Series IP Telephones*.

Weather application parameters that are applicable for the touchscreen phones only - WEATHERAPP, WMLPORT, WMLPROXY.

Web access application parameters - SUBSCRIBELIST, TPSLIST, WMLEXCEPT, WMLHELPSTAT, WMLHOME (Mandatory), WMLIDLETIME, WMLIDLEURI, WMLPORT, WMLPROXY, WMLSMALL.

World Clock application parameters that are applicable for the touchscreen phones only - WMLPORT, WMLPROXY, WORLDCLOCKAPP.

Related links

Administering Applications and Options on page 142

Setting the Application Status flag

9600 Series IP Deskphones 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 17: Application status flags and their meaning of

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. For touch screen phones, this also means that users cannot assign or remove contact Favorites via the Home screen.

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.

Related links

Administering Applications and Options on page 142

Administering the Avaya A Menu

The Avaya A 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 A Menu.

A Home screen replaces the A Menu for touch screen deskphones only for access to menu options and settings, log out, Bluetooth setup, and touch screen cleaning. The Home screen also displays WML applications, Favorite contact speed dial buttons, Avaya applications such as the World Clock and Weather, and a calculator. For more information on administration of touch screen deskphones, see Special Administration for Touchscreen deskphones on page 146. The addition of touch screen models requires that you use the *AvayaMenuAdmin.txt* file to specify the WML applications you want the deskphone to display on the Home screen. These applications are displayed in order from left to right, going to a second page if necessary.

Important:

You must set the system parameter AMADMIN in the 46xxsettings file for Avaya A Menu to work with WML applications. The *AvayaMenuAdmin.txt* file must be a Unicode file to be properly processed by the phones. You can create a Unicode version of this file using Notepad or most text editors. Select *Encoding* and *Unicode*.

If WML applications are installed and the system parameter AMADMIN is set in the settings file:

- The WML applications appear in the first-level A Menu as specified in the *AvayaMenuAdmin* file, as shown in Figure 1 on page 146.
- The first level A Menu on all 9600 Series IP deskphones except touch screen deskphones includes a single entry (Phone Settings) that leads to a screen containing choices for Options & Settings and Network Information. For touch screen phones, the Home screen shows a Settings option that leads to an Options & Settings menu.
- The Phone Settings screen is essentially the current Options and Settings menu, with the addition of Network Information, as shown in Figure 2 on page 147.

If WML applications are installed and the system parameter WMLHOME is set in the settings file, the Avaya A Menu is identical to the pre-Release 1.2 A Menu.

If WML applications are not installed, the A Menu is the same as the current Options & Settings menu, with the addition of Network Information, 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 file when you want to display multiple WML applications on the Avaya A Menu. For more information, see Main Avaya Menu with WML Applications Administered on page 146 and Administering the Avaya Menu with WML applications on page 147 in this chapter.
- Set the system parameter WMLHOME in the settings 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.

Related links

Administering Applications and Options on page 142

Special Administration for Touchscreen Deskphones

The 9621G, 9641G, and 9670G are touch-based phones and use a touch-based Home screen instead of the Avaya menu that other 9600 Series IP deskphones use. Using the home screen, users can gain access to deskphone options and settings, special Avaya applications such as a World Clock, Calculator and Weather, Contact Favorites, and any WML applications you might administer. The Home screen can display up to four WML applications. If you have configured more than four applications, users can gain access to all WML applications through **More**. For information about display characteristics and icons, see How the Home screen displays WML applications on page 149. If the deskphone does not have any WML application, the deskphone might show a single WML Browser item, provided the system parameter WMLHOME is set with a value. For more information about Avaya Menu elements like those for WML applications and exceptions for 9670G or other touchscreen deskphone, see Administering the Avaya “A” Menu on page 145.

Related links

Administering Applications and Options on page 142

Administering WML applications on the Avaya Menu

Administering AMADMIN provides direct links to one or more WML applications. As the figure on page 146 shows, the first level Avaya Menu includes entries for three (sample) WML applications, a Phone Settings menu choice for telephone options and settings, and the telephone log out.

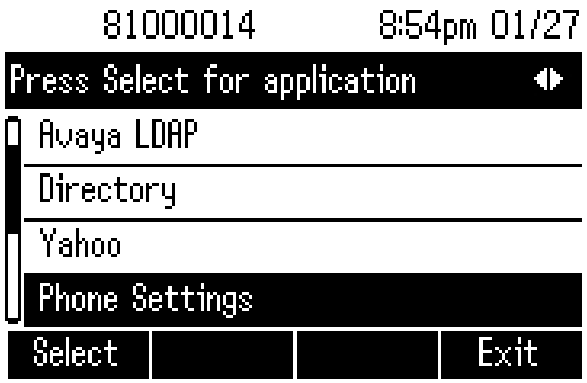


Figure 1: Avaya Menu with WML applications installed as the first three options

If at least one WML application is administered, the administrator can choose to specify the order in which the WML applications and the built-in applications are presented. Any built-in applications

that are not specifically administered in the WML Administration file are automatically appended to the end of the administered list, in the following order:

- Phone Settings
- Log Out
- About Avaya IP Deskphone

If you select an application and press **Select** or **OK**, the application is run. If the Phone Settings application is listed, the deskphone displays Choice Indicator on the Title Line. If you press the Left or Right Navigation buttons, the deskphone displays the Phone Settings screen. If you select Phone Settings, the deskphone displays the Phone Settings menu as follows.

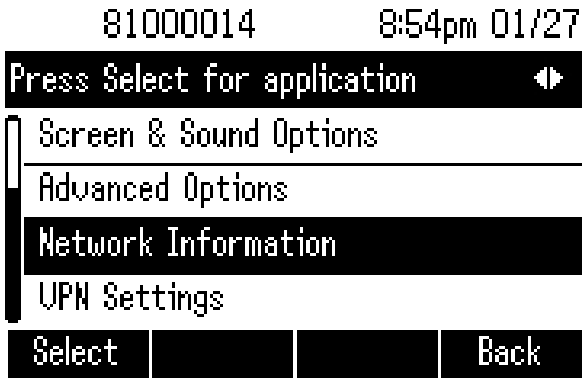


Figure 2: Second Level Avaya Menu - Phone Settings Screen

Related links

Administering Applications and Options on page 142

Administering the Avaya Menu with WML applications

About this task

Administer the AMADMIN parameter in the 46xxsettings file to point to a URL where the AvayaMenuAdmin.txt file resides.

Important:

The `AvayaMenuAdmin.txt` file must be a Unicode file to be properly processed by the phones. You can create a Unicode version of this file using Notepad or most text editors. Select *Encoding* and Unicode.

Note:

Use the `AvayaMenuAdmin.txt` file to specify the WML applications to appear on Home screen of the touch screen models.

Then specify objects for the Avaya Menu through the Avaya Menu Administration file, `AvayaMenuAdmin.txt`. Each administered object, up to the maximum of 12, must have valid, non-null parameter data:

AMTYPExx One of six options: 01 = URI, 02 = the local “Phone Settings” sub-application, 03 = local Log Off sub-application, 04 = the About Avaya IP Deskphone screen, 05 = Guest Login application, 06 = My Pictures application. Touch screen telephones ignore all AMTYPE values except “1”. If the AMTYPE for an associated administered object is “01”, the additional three parameters must have valid, non-null data for the object to be properly administered:

AMLBLxx The label displayed to the user for this object, up to 16 UTF-16 characters, shown left-justified unless spaces precede the label value to center the label.

AMDATAxx A URI of up to 255 ASCII characters, without spaces.

AMICONxx For touchscreen models only, any number, *N*, from 1 to 25. The touch screen deskphone will use the *Nth* icon presented in the table on page 149 on the Home screen in association with the administered WML application. The labels shown in the table on page 149 are suggestions. The touch screen deskphone uses the label you specify in the AMLBLxx parameter.

The *xx* in these three parameters is a two-digit integer from 01 to 12 inclusive, including a leading zero if applicable. If AMTYPE*xx* is 01, *xx* must be the same for each of the three parameters for an Avaya Menu entry to be displayed and associated with the administered data. If AMTYPE*xx* is 02, 03 or 04, any AMLBL*xx* or AMDATA*xx* data is ignored if provided.

If a given administered object has null or invalid data in any of the required associated parameters, that object is completely ignored. To list an AMTYPE01 entry on the Avaya Menu, all three associated parameters must be non-null with valid data. For example, an AMTYPE of “00” is considered invalid.

Do not administer more than nine URIs. You cannot specify a telephone number as a TYPE (unlike the 9610).

In case of duplicate data in the settings file, the last entry is retained. For example, if two consecutive lines in the Avaya Menu Administration file are:

```
AMLBL01=ABCD

AMLBL01=WXYZ
```

then the user sees “WXYZ” as the label for the first WML application. This example assumes the rest of the administration is correct.

If no `AvayaMenuAdmin.txt` file is available, or if the file does not contain at least one valid type 1 (URI) object, the deskphone displays Release 1.0/1.1 Avaya Menu shown in**TERRY*x—ref table**is instead.

Note:

For touchscreen deskphones only, non-WML entries in the AvayaMenuAdmin.txt file are ignored.

Related links

Administering Applications and Options on page 142

How the Home screen displays WML applications

The following table shows the icons, suggested description(s), and numbering to use to specify the WML applications you want the Home screen to display.

Table 18: Home Screen WML Application Icons/Labels

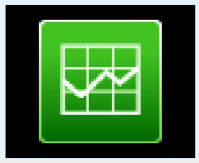
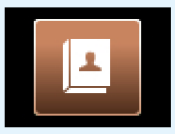
To Display This Icon:	Set AMICONxx to this Label Number (xx value shown below)	Suggested Label (specify in AMBLxx)
	1	Alarm Clock/Wakeup Call
	2	Business data/Sales/Data Analysis
	3	Calendar
	4	Communications
	5	Control (remote, ...)
	6	Directory
	7	Document/Folders/Notes

Table continues…

To Display This Icon:	Set AMICONxx to this Label Number (xx value shown below)	Suggested Label (specify in AMBLxx)
	8	Emergency/Assistance
	9	Food/Restaurant
	10	Financial Information
	11	Front Desk
	12	Help/Site Help/Feature Help
	13	Guard Desk
	14	Information
	15	Inventory
	16	Location/Map

Table continues…

To Display This Icon:	Set AMICONxx to this Label Number (xx value shown below)	Suggested Label (specify in AMBLxx)
	17	Messages
	18	Network
	19	Person/People information
	20	Security/Security Camera
	21	Tickets
	22	Valet Service
	23	Video/TV
	24	Slideshow
	25	Room Service

Related links

[Administering Applications and Options](#) on page 142

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=
```

Related links

Administering Applications and Options on page 142

Administering guest users

About this task

A guest user is a person who logs into a 9600 Series IP deskphone 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. For more information on the parameters, see 9600 Series H.323 customizable system parameters on page 71.

Related links

Administering Applications and Options on page 142

Administering visiting users

About this task

A visiting user is anyone who uses a 9600 Series 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 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 17.

Related links

Administering Applications and Options on page 142

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 19: 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

Table continues…

Shortest Timer	Middle Timer	Longest Timer	Operation
			the phone displays a screen saver on the SCREENSAVERON value.

Note:

You can administer the Backlight Off icon on a 9600 Series 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.

Related links

Administering Applications and Options on page 142

Glossary

802.1X	An authentication method for a protocol requiring a network device to authenticate with a back-end Authentication Server before gaining network access.
CA	Certificate Authority, the entity which issues digital certificates for use by other parties.
CLAN	Control LAN, a type of Gatekeeper circuit pack.
CNA	Converged Network Analyzer, an Avaya product to test and analyze network performance. Applies to IPv4 only. This feature is not supported in Release 6.2 and later.
DHCP	Dynamic Host Configuration Protocol, an IETF protocol used to automate IP Address allocation and management.
Digital Certificate	The digital equivalent of an ID card used in conjunction with a public key encryption system. Digital certificates are issued by a trusted third party known as a “Certificate Authority” (CA) such as VeriSign (www.verisign.com). The CA verifies that a public key belongs to a specific company or individual (the “Subject”), and the validation process the public key goes through to determine if the claim of the subject is correct and depends on the level of certification and the CA.
Digital Signature	A digital signature is an encrypted digest of the file being signed. The file can be a message, a document, or a driver program. The digest is computed from the contents of the file by a one-way hash function such as MD5 or SHA-1 and then encrypted with the private part of a public or private key pair. To prove that the file was not tampered with, the recipient uses the public key to decrypt the signature back into the original digest, recomputes a new digest from the transmitted file and compares the two to see if they match. If they do, the file has not been altered in transit by an attacker.
DNS	Domain Name System, an IETF standard for ASCII strings to represent IP addresses. The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP addresses.

EAP-TLS	Extensible Authentication Protocol, or EAP, is an authentication framework frequently used in wireless networks and Point-to-Point connections. EAP is defined in RFC 3748. EAP-Transport Layer Security (EAP-TLS), defined in RFC 5216, is an IETF open standard protocol, with strong security used by wireless vendors. EAP-TLS uses PKI to secure communication to a RADIUS authentication server or another type of authentication server.
H.323	H.323 is a TCP/IP-based protocol for VoIP signaling. The H.323 standard provides a foundation for audio, video, and data communications across IP-based networks, including the Internet. H.323 is an umbrella recommendation from the International Telecommunications Union (ITU) that sets standards for multimedia communications over Local Area Networks (LANs) that do not provide a guaranteed Quality of Service (QoS).
HAC	Hearing Aid Compatibility, an Federal Communications Commission (FCC), part of the United States government Part 68 standard for handset equalization for interoperability with t-coil enabled hearing aid devices.
IKE	Internet Key Exchange Protocol, RFC 2409, which is now replaced by IKEv2 in RFC 4306.
IPsec	A security mechanism for IP that provides encryption, integrity assurance, and authentication of data. Applies only to IPv4.
LLDP	Link Layer Discovery Protocol. All deskphones with an Ethernet interface support the transmission and reception of LLDP frames on the Ethernet line interface in accordance with IEEE standard 802.1AB.
MAC	Media Access Control, ID of an endpoint.
NAT	Network Address Translation, a mechanism by which IP addresses are mapped from one address space to another, and in which UDP and TCP port numbers are remapped to allow multiple devices to share the same IP address without port number conflicts.
PSTN	Public Switched Telephone Network, the network used for traditional telephony.
Quality of Service	Quality of Service (QoS) is used to refer to several mechanisms intended to improve audio quality over packet-based networks.
RSA	Rivest-Shamir-Adleman: A highly secure asymmetric cryptography method developed by RSA Security, Inc. that uses a public and private key pair. The private key is kept secret by the owner and the public key is published, usually in a digital certificate. Data is encrypted using the public key of the recipient, which can only be decrypted by the private key of the recipient. RSA is very computation intensive, thus it is often used to

	encrypt a symmetric session key that is then used by a less computationally-intensive algorithm to encrypt protocol data during a “session”. You can also use RSA for authentication by creating a digital signature, for which the private key of the sender is used for encryption, and the public key of the sender' is used for decryption.
RTCP	RTP Control Protocol, monitors quality of the RTP services and can provide real-time information to users of an RTP service.
SCEP	Simple Certificate Enrollment Protocol, used to obtain a unique digital certificate.
Session Initiation Protocol	Session Initiation Protocol (SIP) is an alternative to H.323 protocol used for VoIP signaling.
SNTP	Simple Network Time Protocol. An adaptation of the Network Time Protocol used to synchronize computer clocks in the internet.
TFTP	Trivial File Transfer Protocol, used to provide downloading of upgrade scripts and application files to certain IP telephones.
VoIP	Voice over IP, a class of technology for sending audio data and signaling over LANs.
VPN	Virtual Private Network, a private network constructed across a public network such as the Internet. A VPN can be made secure, even though the network uses using existing Internet connections to carry data communication. Security measures involve encrypting data before sending data across the Internet and decrypting the data at the other end. To add an additional level of security, you can encrypt the originating and receiving network address.
WML	Wireless Markup Language, used by the IP phones Web Browser to communicate with WML servers.

Index

Numerics

46xxsettings
    JITC parameters 20
802.1X 110
9600 Series IP deskphones
    customizing applications and options 142
9600 Series IP Deskphones
    overview 10

A

administering 130
    DIFFSERV 41
    guest user 154
    input methods 117
    language selection 117
    QOS 41
    RSVP 40
    visiting users
        administering 154
    VLAN 102
Administering deskphones for call center operation 131
Administering Features 47
administration
    call server 39
    checklist 11
    DHCP and file servers 50
    parameters 18
    responsibilities 10
administration, ... 14
administrator
    responsibilities 10
aliasing 25
application file
    upgrade script file
        application file 66
Application Icons/Labels, for Home Screen 149
Application Status Flag (APPSTAT) 143
Application Status Flags and Their Meaning 143
APPSTAT 143
Audio equalization 130
Auto-answer 133
Auto Hold administration 45
Auto select any idle appearance administration 47
Avaya 145
Avaya Menu Administration 147
Avaya Menu Administration File Template 152
Avaya Menu with WML Applications 146

B

Backup 137
Backup, Options and Non-Password Parameters Saved 138
Backup/Restore 135
Backup/restore processing 60
Backup File Formats 137

C

Call Center operation, administering 131
call server
    administration 39
    requirements 39
call servers
    IP interface and addresses 40
call transfer
    considerations 43
certificate, revocation 16
certificates 16
certificates, OCSP 16
certificates, revocation 16
certificates, security 16
certificates, usage 16
checklist
    initial administration 11
Conference/Transfer on Primary Appearance administration 47
considerations during call conferences 44
Coverage Path administration 45, 47
customizable options 70
custom screen saver, administering 130

D

data precedence
    parameters 15
DHCP
    generic setup
        DHCP 51
DHCP, Parameters Set by 55
DHCP Generic Setup 55
DHCP options 52, 58
DHCP server 27
dialing methods 118
DIFFSERV
    administering 41
DNS addressing 104
downloads
    certificate files 16
    language files 16
    settings configuration files 16
    upgrade configuration files 16

E

EAP-TLS 105
authentication 106
phones using MD5 107
scenarios 107
without 802.1 authentication 109
EC500 administration 45
enabling
SCEP support 105
Enhanced Conference Features administration 45, 47
error conditions 25

F

Far End Mute administration 47
Feature administration for all other deskphones 48
Feature Administration for Avaya Communication Manager 45
Feature Numbers for Assigning Softkeys 122
Feature-Related System Parameters, administering on CM 45
Features, Administering on Softkeys 122
files
configuration 16
settings
language 16

G

General Download Process 65
GROUP parameter 68

H

hardware requirements 26
Home screen
managing applications 119
Home Screen WML Application Icons/Labels 149
HTTP redirect 60

I

idle timer settings 155
IEEE 802.1D and 802.1Q 29
IEEE 802.1Q 41
IEEE 802.IQ QoS parameters 41
initialization process 15
installation
required network information 27
intended audience 8
IP interface and addresses
call servers 40
IPv4 and IPv6 operation 62
IPv6 62
IPv6 Limitations 64

L

legal notices .....
Link Layer Discovery Protocol (LLDP) 112
local administrative
options 116

M

mode, JITC 19

N

NAT 41
network assessment 26
network considerations
audio quality display 30
generic setup
DHCP 29
IP address 29
IP address lists 30
ping 29
port utilization 31
QoS 29
quality of service 29
SMIv2 28
SNMP 28
Station Number Portability 30
TCP/UDP 31
Time-to-Service (TTS) 37
traceroute 29

O

On-Hook Dialing administration 45
options
local administrative 116
options, customizing 142
overview
9600 Series IP Deskphones 10
JITC security 19

P

parameters
administration options 18
data precedence 15
parameters, customizable 71
parameters in real-time 30
Parameters Saved During Backup 138
phone
administration 45
call server initialization 17
file server initialization 16
initialization to DHCP server 16
network initialization 15

port selection
UDP 40
purpose 8

Q

QoS
administering 41
IEEE 802.1Q 41

R

Registration and Authentication 37
related courses 9
related documentation 8
required network information 27
requirements
call server 39
hardware 26
server 27
Restore 140
Restore/Backup 135
Restrict Last Call Appearance administration 47
RSVP
administering 40

S

SCEP support
enabling 105
screen saver, administering 130
Secure Shell Support 37
security 35
security, compliance 19
security, FIPS 19
Send All Calls (SAC) administration 47
server
requirements 27
settings file 67
SNMP
enablement 28
Softkeys, Administering Features on 122
software prerequisites 50
SRTP 31
SSO logon 101
SSON, Option 242, configuring 55
station administration 47
Station Form Administration Results Chart 48
Station Number Portability
IP address lists 30
supplicant operation, 802.1X 111
support 9
switch compatibility and aliasing IP telephones 25
System Parameters 45
system parameters, customizable 71

T

TLS 31

U

UDP
port selection 40
UDP/TCP Port Utilization 31
unnamed registration 17
upgrading 67

V

VLAN
administering 102
VLAN Default Value 103
VLAN detection 103
VLAN tagging 102

W

Wideband Audio administration 45
Wireless Headset 132
WML Application Display, on Home screen 149
WML browser 121
WML browser properties 121