Administering Avaya H100-Series Video Collaboration Stations

Release 1.0.2
April 2016

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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 a 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 IF YOU PURCHASE A 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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

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

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

License types

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage

Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

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

The following applies 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

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Regulatory Statements

Australia Statements

Handset Magnets Statement

Danger:

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

Handset Amplification Statement

Enabling the amplified capability will result in the handset not being compliant to all Australian S004 requirements, but will allow the handset to be fully compliant with United States 508 Section 1194.23(f) Standards.

Industry Canada (IC) Statements

RSS Standards Statement

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

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

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

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

Radio Transmitter Statement

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

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

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

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

Radiation Exposure Statement

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

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

Japan Statements

Class B Statement

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

Denan Power Cord Statement

Danger:

Please be careful of the following while installing the equipment:

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

警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

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

México Statement

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

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

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

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

Power over Ethernet (PoE) Statement

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

Taiwan Low Power Radio Waves Radiated Devices Statement

802.11b/802.11g/BT:

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

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

802.11b/802.11g/BT 警語：

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

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

U.S. Federal Communications Commission (FCC) Statements

Compliance Statement

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

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

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

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

Class B Part 15 Statement

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

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

Radiation Exposure Statement

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

EU Countries

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

General Safety Warning

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

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

Trademarks

Contents

Chapter 1: Introduction

Purpose

This document contains information about how to perform Avaya H100-Series Video Collaboration Stations administration tasks including how to use management tools, how to manage data and security, and how to perform periodic maintenance tasks.

Intended audience

This document is intended for people who perform Avaya H100-Series Video Collaboration Stations system administration tasks, such as user management, device configuration, and device upgrade and maintenance.

Related resources

Documentation

Title	Use this document to:	Audience
Overview		
Avaya H100-Series Video Collaboration Stations Overview and Specification	See characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security and licensing requirements of the Avaya H100-Series Video Collaboration Stations.	For people who want to gain a high-level understanding of the Avaya H100-Series Video Collaboration Stations features, functions, capacities, and limitations.
Implementing		

Table continues…

Title	Use this document to:	Audience
Installing and Maintaining Avaya H100-Series Video Collaboration Stations	See information about preparing the Avaya H100-Series Video Collaboration Stations for installation, deployment, initial administration, maintenance and troubleshooting.	For people who install and maintain the Avaya H100-Series Video Collaboration Stations.
Deploying Avaya Aura® Session Manager	See the installation procedures and initial administration information for Avaya Aura® Session Manager.	For people who install, configure, and verify Avaya Aura® Session Manager on Avaya Aura® System Platform.
Upgrading Avaya Aura® Session Manager	See upgrading checklists and procedures.	For people who perform upgrades of Avaya Aura® Session Manager.
Deploying Avaya Aura® System Manager on System Platform	See the installation procedures and initial administration information for Avaya Aura® System Manager.	For people who install, configure, and verify Avaya Aura® System Manager on Avaya Aura® System Platform at a customer site.
Deploying Avaya Aura® Conferencing: Basic Installation	See the installation procedures and initial administration for Avaya Aura® Conferencing.	For people who install and configure Avaya Aura® Conferencing.
Installation guide for Avaya Scopia® Management	See the installation procedures and initial administration for Avaya Scopia®.	For people who install and configure Avaya Scopia®.
Administering		
Administering Avaya Aura® Session Manager	See information about how to perform Avaya Aura® Session Manager administration tasks including how to use management tools, how to manage data and security, and how to perform periodic maintenance tasks.	For people who perform Avaya Aura® Session Manager system administration tasks.
Administering Avaya Aura® System Manager for Release 7.0.1	See information about how to perform Avaya Aura® System Manager administration tasks including how to use management tools, how to manage data and security, and how to perform periodic maintenance tasks.	For people who perform Avaya Aura® System Manager administration tasks.
Administering Avaya Aura® Conferencing	See information about how to perform Avaya Aura® Conferencing administration tasks.	For people who perform Avaya Aura® Conferencing administration tasks.
Avaya Scopia® Management Administrator Guide	See information about how to perform Avaya Scopia® administration tasks.	For people who perform Avaya

Table continues…

Title	Use this document to:	Audience
		Scopia® administration tasks.
Maintaining		
Maintaining Avaya Aura® Session Manager	See information about the maintenance tasks for Avaya Aura® Session Manager.	For people who maintain Avaya Aura® Session Manager.
Troubleshooting Avaya Aura® Session Manager	See information for troubleshooting Avaya Aura® Session Manager, resolving alarms, replacing hardware, and alarm codes and event ID descriptions.	For people who troubleshoot Avaya Aura® Session Manager.
Using		
Using Avaya H175 Video Collaboration Station	See capabilities of the Avaya H175 Video Collaboration Station and to learn about how various features work.	For people who want to learn how to use Avaya H175 Video Collaboration Station features.
Avaya H175 Video Collaboration Station Quick Reference	See frequently used tasks.	For people who want to learn how to use Avaya H175 Video Collaboration Station features.

Finding documents on the Avaya Support website

About this task

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

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

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

8. Click **Enter**.

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: Avaya H100-Series Video Collaboration Stations overview

The Avaya H100-Series Video Collaboration Stations are SIP-based VoIP HD video deskphones that enterprises can use for audio, video, and conference communications. The Collaboration Stations combine the functionality of a business telephone and an executive video conference system.

You can use the Collaboration Station as:

- A traditional video phone by mounting the camera on the device.
- A high-end conference system by mounting the camera on an external monitor.

You can also connect the Collaboration Station and your personal computer to an external monitor to get the picture-in-picture (PiP) functionality as shown in the image below.

Related links

Specifications on page 13
Product compatibility on page 16
Administrator responsibilities on page 16
Administration methods on page 17
Initial administration checklist on page 18
Setting the search string length for Microsoft Exchange Server on page 19

Specifications

Specification	Category	H175
Hardware	Display	7–inch IPS LCD display, capacitive touchscreen, 16 M colors, and a resolution of 1280 x 800 px.
	Audio	• Wideband audio through handset, headset, and speakerphone. • Supported audio codecs are G.711 A-law/mu-law, G.722, G.729A/AB, G. 726-32.
	Video	• Full HD, two way video calls up to 1080p 30 frames per second. • H.264 AVC baseline and high profile. • Support external monitors with resolutions up to 1080p. • Zero latency, display pass-through with Picture-in-Picture functionality for sharing an external monitor with a computer. • User control for video window size and position. • Dynamic adaptation of incoming bit-rate to the current video window size for bandwidth saving.
	Camera	• Detachable Full HD video camera (1920x1080) optimized for office use. • Bright, f2.0 lens for a superior performance in low light.

Table continues…

		• Camera that can be mounted on the device or on an external monitor. • Mechanical privacy shutter. • Activity LED.
	Handset	• Wireless handset, which is available in specific countries, supports DECT 6.0 and has call control, mute, and volume buttons. • Optional wired handset.
	Physical security	Kensington security slot.
	Physical buttons and LEDs	• Dialpad: 0-9, *, and #. • Volume up and volume down buttons. • Audio mute and video block buttons. • Speakerphone and headset buttons. • Message Waiting Indicator LED. • LED touch buttons.
	Connectors	• RJ45 primary Gigabit Ethernet (10/100/1000 Mbps) PoE LAN port. • RJ45 secondary Gigabit Ethernet (10/100/1000 Mbps) port for personal computer. • USB dedicated camera port. • USB 2.0 charging port with up to 1.5 A power to rapidly recharge smartphones and tablets. • Two USB 2.0 general purpose ports. • USB 2.0 micro AB port. • Digital display video output port capable of supporting a monitor with up to 1080p. • Digital display input port capable of handling digital video from a personal computer for picture-in-picture video overlay support. • RJ9 analog handset port. • RJ9 analog headset port. • SD card slot is not currently supported. • 48 V AC power supply.
	Processor	Freescale i.Mx6 1.0 GHz quad-core ARM Cortex-A9 processor.
	Storage	4GB eMMC flash memory configured as SLC.
	Memory	2 GB of RAM.
Connectivity	Ethernet	Gigabit Ethernet.
	Wi-Fi	Dual-band, 2.4 GHz and 5 GHz, 802.11a/b/g/n.

Table continues…

	Bluetooth	Supports: • Bluetooth 4.0. • Headset profile.
Power	Ethernet	• IEEE 802.3at. • Single Port PoE injector (SPPoE).
	AC power	External 30 W AC power adapter.
Accessory support	-	• USB headset, keyboard, and mouse. • Bluetooth HID-keyboard and mouse. • Bluetooth headsets.
Software features	-	• Android 4.3 operating system. • Avaya Aura® features. - Audio and video call management. - Advanced call management, such as call forwarding, call transfer, call park, and bridged call appearances. • IP Office v10.0 features. - Audio and video call management. - Synchronize user contacts with Avaya one-X® Portal. • Audio and video call with Avaya Scopia® Elite MCU and Avaya Aura® Conferencing with roster control. • Microsoft Exchange Server calendar and contacts integration. - Microsoft Exchange Server calendar integration with built-in click-to-call support. • Contact app - Synchronize contacts with Microsoft Exchange Server . - Synchronize user contacts with Avaya Aura® System Manager. - Synchronize user contacts with Avaya one-X® Portal. • Publish and display presence status with Avaya Aura® Presence Services integration. • Enhanced user interface shared with Avaya Communicator 2.0 optimized for touchscreen. • HTML 5 browser with built-in click-to-call support. • History, Calculator, and Alarm clock apps. • Online help.
Security		• Screen lock facility. • 802.1x EAP-TLS and EAP-MD5 over the Ethernet interface.

Table continues…

		• Wi-Fi WEP, WPA/WPA2 PSK, and 802.1x EAP, where for 802.1x EAP following features are supported: - EAP-PEAP with MSCHAPV2 and EAP-GTC as phase 2 authentication methods. - EAP-TLS. - EAP-TTLS with MSCHAP, MSCHAPV2, and EAP-GTC as phase 2 authentication methods. - EAP-PWD. • Trusted certificate repository configured through the settings file to be used by all applications. • Android built in certificates are used in addition to trusted certificates for the browser and Microsoft Exchange Server. • Identity certificate generation using SCEP. • Support SIP signaling over TLS. • Media encryption (SRTP) using AES-128 and AES-256. • Supports SRTCP (authentication only). • User information, such as MS Exchange credentials, call logs, and browser history, is erased when a new user logs in.

Related links

Avaya H100-Series Video Collaboration Stations overview on page 12

Product compatibility

For the latest compatibility information about the Avaya H175 Video Collaboration Station with:

- Other products, see Compatibility Matrix.
- Headsets, see DevConnect Portal.

Related links

Avaya H100-Series Video Collaboration Stations overview on page 12

Administrator responsibilities

An administrator can perform the following tasks:

- Manage network configurations.
- Provision features.
- Manage accounts.

- Manage app-specific configurations.
- Manage upgrade configurations.
- Manage security configurations.

Related links

Avaya H100-Series Video Collaboration Stations overview on page 12

Administration methods

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

Method	Can administer					
	IP addresses	Ethernet Interface	Tagging and VLAN	Network Time Server	Quality of Service	Application-specific parameters
DHCP	✔	✔	✔	✔	—	✔
LLDP	✔	✔	✔	—	—	—
Settings file	—	✔	✔	✔	✔	✔
Avaya Aura® Session Manager	—	—	✔	—	✔	—
Settings app on the device	✔	✔	✔	—	—	✔

Precedence of the methods

Most of the parameters are configurable through multiple methods. If you configure a parameter through more than one method, the device applies the settings of the method that has a higher precedence. For the parameters that are not backed up through PPM, the non-default value has the highest precedence. The following list shows the precedence of the methods in the highest to lowest order:

1. Settings app on the device. There is an exception of DHCP getting a higher precedence when:
   - IP address is set through DHCP.
   - USE_DHCP parameter is set to 1 to assign a higher priority to DHCP.
2. Avaya Aura® Session Manager.
3. Settings file.
4. DHCP.

5. LLDP. There is an exception of LLDP getting a higher precedence than the settings file and DHCP when the layer 2 parameters, such as L2QVLAN, L2Q, L2QAUD, L2QVID, L2QSIG, DSCPAUD, DSCPSIG, DSCPVID, and PHY2VLAN are set through LLDP.

Note:

The parameter resets to its default value when it is removed from the settings file and is not defined through any other source.

Related links

Avaya H100-Series Video Collaboration Stations overview on page 12

Initial administration checklist

No.	Task	Reference	✔
1	Ensure that the device is set up, assembled, and operating.	For installing instructions that include steps for connecting the wireless or the wired handset, attaching the camera, and powering up the device, see *Installing and Maintaining Avaya H100-Series Video Collaboration Stations*.	
2	Ensure that the initial configuration parameters are provisioned through the settings file, DHCP, LLDP, or the device interface.	For provisioning the initial configuration parameters, such as the file server address, SIP registration details, country code for wireless handset, and conferencing URI, see *Installing and Maintaining Avaya H100-Series Video Collaboration Stations*.	
3	Set the search string length for Microsoft Exchange Server if the deskphone is synchronized to an Exchange Server.	See Setting the search string length for Microsoft Exchange Server on page 19.	
4	Ensure that the SIP Endpoint Managed Transfer parameter is set to yes in the Communication Manager settings to enable the advanced ad-hoc conferencing.	See the feature-related parameter settings in *Administering Avaya Aura® System Manager for Release 7.0.1*.	

Related links

Avaya H100-Series Video Collaboration Stations overview on page 12

Setting the search string length for Microsoft Exchange Server

About this task

Use this procedure to set the minimum length of the search string for Microsoft Exchange Server 2010 to three characters.

Procedure

1. Open the `web.config` file located in the folder `\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Sync\`.
2. In the appSettings section, add `<add key="MinGALSearchLength" value="3"></add>`.

Related links

Avaya H100-Series Video Collaboration Stations overview on page 12

Chapter 3: Configuration through the DHCP options

DHCP overview

The Avaya H100-Series Video Collaboration Stations connect to the DHCP server during the boot up. You can configure the DHCP server to provide the following information to the device:

- IP address
- Subnet mask
- IP address of the router
- IP address of the HTTP or HTTPS file server
- IP address of the SNTP server
- IP address of DNS

DHCP options configuration

Ensure that the following options are set in the DHCP server. Provision options that are specified in the following table only as configuring additional options might cause unexpected result and the device to ignore the DHCP server.

Option	Description
Option 1	Specifies the subnet mask of the network.
Option 3	Specifies the gateway IP address list. The list can contain up to 127 total ASCII characters. Separate more than one IP address with commas with no intervening spaces.
Option 6	Specifies the DNS server address list. The list can contain up to 127 total ASCII characters. Separate more than one IP address with commas with no intervening spaces. The deskphone supports DNS and the dotted decimal addresses. The deskphone attempts to resolve a non-ASCII-encoded dotted decimal IP address by checking the

Table continues…

Option	Description
	contents of DHCP Option 6. At least one address in option 6 must be a valid, nonzero, dotted decimal address, otherwise the DNS address fails.
Option 12	Specifies the host name. AVohhhhhh, where: • o is one of the following values based on Object Unique Identifier (OUI) derived from the first three octets of the deskphone MAC address: - A if OUI is 00-04-0D - B if OUI is 00-1B-4F - E if OUI is 00-09-6E - L if OUI is 00-60-1D - T if the OUI is 00-07-3B - X if the OUI is anything else • hhhhhh are the ASCII characters for the hexadecimal representation of the last three octets of the deskphone MAC address.
Option 15	Specifies the domain name. The domain name is required to resolve DNS names into IP addresses. Configure this option if you use a DNS name for the HTTP server. Otherwise, you can specify a domain as part of customizing the HTTP server. This domain name is appended to the DNS addresses specified in option 6 before the deskphone attempts to resolve the DNS address. The deskphone queries the DNS address in the order they are specified in option 6. If there is no response from an address, the deskphone queries the next DNS address. As an alternative to administering DNS by DHCP, you can specify the DNS server and domain name in the HTTP script file. If you use the script file, you must configure the DNSSRVR and DOMAIN parameters so that you can use the values of these parameters in the script. **Note:** Administer option 6 and option 15 appropriately with DNS servers and domain names respectively.
Option 42	Specifies the SNTP IP address list. List servers in the order of preference. The minimum length is 4 and the length must be a multiple of 4.
Option 43	Specifies the encapsulated vendor-specific options that clients and servers use to exchange the vendor-specific information. Option 43 is processed only if the first code in the Option is 1 with a value of 6889. All values are interpreted as strings of ASCII characters that are accepted with or without a null termination character. Any invalid value is ignored and the corresponding parameter value is not set. For information on codes for this parameter, see Codes for option 43 on page 23.
Option 51	Specifies the DHCP lease time. If this option is not received, the DHCPOFFER is not accepted. Assign a lease time of six weeks or greater. If this option has a value of

Table continues…

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

Parameters such as HTTPSRVR and SIP_CONTROLLER_LIST support values with lengths up to 255 octets, but you must set shorter values when you are setting them through DHCP.

Related links

Codes for Option 43 on page 23
DHCP lease time on page 23
Parameter configuration through DHCPACK on page 24

Codes for Option 43

The supported codes for Option 43 and the corresponding parameters are as follows:

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

Related links

DHCP options configuration on page 20

DHCP lease time

The DHCP standard states that when a DHCP lease expires, the device should immediately cease using its assigned IP address. However, if the network has problems and the only DHCP server is centralized or if the DHCP server itself has problems, the device will not receive responses to its request for a renewal of the lease. In this case the device is not usable until the server can respond. Configure system such that once the IP address is assigned to the device, the device continues using that address after the DHCP lease expires, until a conflict with another device is detected.

The system parameter DHCPSTD allows an administrator to specify that the device will either:

- Comply with the DHCP standard by setting DHCPSTD to 1.

- Continue to use its IP address after the DHCP lease expires by setting DHCPSTD to 0.

The latter case is the default. If the default is invoked, after the DHCP lease expires the deskphone continues to broadcast DHCPREQUEST messages for its current IP address, and it sends an ARP Request for its own IP address every five seconds.

The messages continue to be sent until the device receives a DHCPACK, a DHCPNAK, or an ARP reply. After receiving a DHCPNAK or ARP reply, the device displays an error message, sets its IP address to 0.0.0.0, and attempts to contact the DHCP server again. Log events are generated for either case.

Depending on the DHCP application you choose, the application might not immediately recycle expired DHCP leases. An expired lease might remain reserved for the original client a day or more. If the client and the DHCP server are in two different time zones, the clocks of the computers are not in sync, or the client is not on the network when the lease expires, there is time to correct the situation.

The following example shows the implication of having a reservation period.

Assume that there are two IP addresses, therefore two possible DHCP leases. Assume that there are three IP devices in the network, two of which are using the two available IP addresses. When the lease for the first two devices expires, the third device cannot get a lease until the reservation period expires. Even if the other two devices are removed from the network, the third device remains without a lease until the reservation period expires.

Related links

DHCP options configuration on page 20

Parameter configuration through DHCPACK

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

Table continues…

Parameter	Set to
ROUTER	Option 3, if received, which might be a list of IP addresses
SNTPSRVR	Option 42

Related links

DHCP options configuration on page 20

DHCP site-specific option

You can set the values of site-specific configuration parameters through a DHCP option. The default DHCP option to set the site-specific configuration parameters is 242. You can also use any option between 128 to 254. Whichever option you select to specify the site-specific configuration, you must specify that option number in the Site-Specific Option Number (SSON) parameter. You can set the SSON parameter through the device interface.

Following is an example of the DHCP 242 option string that specifies the HTTPSRVR and the Voice VLAN that the device must connect to.

HTTPSRVR=10.138.251.67,L2QVLAN=1104

The following table lists the site-specific configuration parameters that you can define for the device.

Parameter	Description
FILE_SERVER_URL	Specifies the list of URL for downloading image and configuration files. This parameter has higher precedence over HTTPSRVR, HTTPPORT, HTTPDIR, TLSSRVR, TLSDIR, and TLSPORT.
HTTPDIR	Specifies the path to prepend to all configurations and data files the device might request when starting up, that is, the path, relative to the root of the HTTP file server, to the directory in which the device configuration and date files are stored. The path may contain no more than 127 characters and may contain no spaces. HTTPDIR is the path for all HTTP operations. The command is "SET HTTPDIR=<path>". In configurations where the upgrade and binary files are in the default directory on the HTTP server, do not use the HTTPDIR=<path>.
HTTPPORT	Destination port for HTTP requests. The default is 80.
HTTPSRVR	IP addresses or DNS names of HTTP file servers used for downloading settings and firmware files during startup. The firmware files are digitally signed, so TLS is not required for security.
ICMPDU	Controls the extent to which ICMP Destination Unreachable messages are sent in response to messages sent to closed ports so as not to reveal information to potential hackers. The default is 1, that is sends Destination Unreachable messages for closed ports used by traceroute.
ICMPRED	Controls whether ICMP Redirect messages are processed. The default is 0, that is, redirect messages are not processed.

Table continues…

Parameter	Description
L2Q	802.1Q tagging mode. The default is 0 for automatic.
L2QVLAN	VLAN ID of the voice VLAN. The default is 0.
PHY1STAT	Controls the Ethernet line interface speed. The default is 1 for auto-negotiate.
PHY2STAT	Controls the secondary Ethernet interface speed. The default is 1 for auto-negotiate.
PROCPSWD	Security string used to access local procedures. The default is 27238.
REUSETIME	Time in seconds for IP address reuse timeout, in seconds. The default is 60 seconds.
SIP_CONTROLLER_LIST	SIP proxy or registrar server IP or DNS addresses that can be 0 to 255 characters, IP address in the dotted decimal name format, separated by commas and without any intervening spaces. The default is null, that is, no controllers.
TLSDIR	Used as path name that is prepended to all file names used in HTTPS GET operations during initialization. The string length can be from 0 to 127.
TLSPORT	Destination TCP port used for requests to https server in the range of 0 to 65535. The default is 443, the standard HTTPS port.
TLSSRVR	IP addresses or DNS names of Avaya file servers used to download configuration files. Firmware files can also be downloaded using HTTPS. **Note:** Transport Layer Security is used to authenticate the server.
VLANTEST	Number of seconds to wait for a DHCPOFFER on a non-zero VLAN. The default is 60 seconds.

Chapter 4: Configuration through the settings file

Settings file overview

You can administer the Avaya H100-Series Video Collaboration Stations centrally through the settings file that Avaya provides with the devices. The settings file is a text file that resides on a file server and contains configuration parameters.

Configuring the settings file

About this task

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

Procedure

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

General parameters

Server addresses and ports parameters

Parameter	Type	Default value	Description
DNSSRVR	String	0.0.0.0	Specifies the DNS server IP addresses in dotted-decimal format, separated by commas with no

Table continues…

Parameter	Type	Default value	Description
			intervening spaces. The range is 0 to 255 ASCII characters including commas.
DOMAIN	String	Null	Specifies a text string that contains the domain name to be used when DNS names in parameter values are resolved into IP addresses. The range is 0 to 255 ASCII characters.
FILE_SERVER_URL	String	Null	Specifies the configured file server URLs for downloading firmware and configuration files. If this parameter is set, then the following parameters are ignored: • HTTPSRVR • HTTPPORT • HTTPDIR • TLSSRVR • TLSSRVRDIR • TLSPORT
HTTPSRVR	String	0.0.0.0	Specifies a list of IP or DNS addresses of the HTTP servers for downloading settings file and firmware during startup procedure. HTTP server addresses can be in dotted decimal or DNS format, and must be separated by commas. The range is from 0 to 255 ASCII characters including commas.
HTTPDIR	String	Null	Specifies the path to prepend to all configurations and data files that the device might request when starting up. The path is relative to the root of the HTTP file server and to the directory in which the configuration and date files are stored. The path can contain no more than 127 characters and must not contain spaces. If an Avaya file server is used to download configuration files over HTTPS, 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. In configurations where the upgrade and binary files are in the default directory on the HTTP server, do not use the HTTPDIR=<path>.

Table continues…

Parameter	Type	Default value	Description
HTTPPROXY	String	Null	Specifies a list of IP or DNS addresses of HTTP proxy servers. If this parameter is not null, the proxy transport address assigned in this parameter is used to set up the HTTP connection as transport protocol for browser, and Exchange account. This parameter is not a URL and must not begin with the text http://., for example, ca.avaya.com:8000.
HTTPEXCEPTIONDOMAINS	String	Null	A HTTP connection as transport layer for the Andorid browser and Exchange account is only set up through the parameter HTTPPROXY, if the right-most part of the domain portion of the Exchange server name and web page name does not match to one of the values in this parameter.
TLSDIR	String	Null	Specifies the path name for HTTPS downloads. The range is from 0 to 127 characters.
HTTPPORT	Numeric	80	Specifies the destination port for HTTP requests. The range is from 0 to 65535.
TLSPORT	Numeric	443	Specifies the destination port for HTTPS requests. The range is from 0 to 65535.
CONFIG_SERVER	String	Null	Specifies the address of the PPM configuration server. If the SIP environment is set up such that the PPM server is at a different location than the SIP proxy server address, the device uses the configuration server address instead. The device will not use the proxy server for PPM. **Note:** This parameter is only supported in an Avaya Aura® environment.
SIP_CONTROLLER_LIST	String	Null	Specifies a comma separated list of IP addresses of SIP proxy or registrar server. The range is from 0 to 255. The list has the following format. host[:port][;transport=xxx], where: • host is an IP address in dotted-decimal format • port is the optional port number. If you do not specify a port number, the system uses the following default values: - 5060 for TCP - 5061 for TLS

Table continues…

Parameter	Type	Default value	Description
			• transport is the optional transport type, tls or tcp. If you do not specify the transport, the system uses TLS as the default type
SIMULTANEOUS_REGISTRATIONS	Numeric	3	Specifies the number of simultaneous Session Manager and Branch Session Manager registrations that the device can maintain. The range is from 1 to 3.
ENABLE_PPM_SOURCED_SIPPROXYSRVR	Numeric	1	Specifies whether to enable PPM as a source of SIP proxy server information. Assign one of the following values: • 0 • 1
SIPDOMAIN	String	Null	Specifies the SIP domain name for registration. The range is from 0 to 255.
SIPPORT	Numeric	5060	Specifies the port the deskphone opens to receive the SIP signaling messages over TCP. This is the listening port when SIP/TCP is used and dual socket is used with Avaya Aura® Session Manager, that is, the CONNECTION_REUSE parameter is 0. You can set this parameter only if the environment is not an Avaya environment. The range is from 1024 to 65535.
SIP_PORT_SECURE	Numeric	5061	Specifies the default SIP port for secure message transfer through TLS. This is the listening port when SIP/TLS is used and dual socket is used with Avaya Aura® Session Manager, that is, the CONNECTION_REUSE parameter is 0. You can set this parameter only if the environment is not an Avaya environment. The range is from 1024 to 65535.
PRESENCE_SERVER	String	Null	Specifies the address and optional port of a single Presence server. The range is from 0 to 255 characters.
MWISRVR	String	Null	Specifies a list of IP or DNS addresses for Message Waiting Indicator Event Server. The range is from 0 to 255 characters. You can set this parameter only if the environment is not an Avaya environment
SNTPSRVR	String	Null	Specifies a list of IP or DNS addresses for the SNTP server. The range is from 0 to 255 characters.

Table continues…

Parameter	Type	Default value	Description
LOGSRVR	String	Null	Specifies the IP or DNS addresses for the Syslog server. The range is from 0 to 255 characters.
RTCPMON	String	Null	Specifies the IP or DNS address for the RTCP monitor. You can set this parameter only if the environment is not an Avaya environment. The range is from 0 to 255 characters.
RTCPMONPORT	Numeric	5005	Specifies the RTCP monitor port number. You can set this parameter only if the environment is not an Avaya environment. The range is from 0 to 65535.
EXCHANGE_SERVER_LIST	String	Null	Specifies a list of IP or DNS addresses for the Microsoft Exchange™ server. The range is from 0 to 255 characters.
CONFERENCE_FACTORY_URI	String	Null	Specifies the conference server URI used to start an Avaya Aura® Conferencing conference call.
SIGNAL_P_CONFERENCE_SIP_HEADER	Integer	1	Specifies whether to enable P-Conference header in SIP 200 OK message sent to the AAC conferencing server. Assign one of the following values: • 1: P-Conference header will be sent • 0: P-Conference header will not be sent
P_CONF_OUTDIAL_PROMPT	Integer	0	Specifies whether the value of P-Conference header should contain true or false for “OutdialPrompt=”. Assign one of the following values: • 1: P-Conference header should contain true for “OutdialPrompt=” • 0: P-Conference header should contain false for “OutdialPrompt=”
P_CONF_FEEDBACK_PROMPTS	Integer	0	Specifies whether the value of P-Conference header should contain true or false for “FeedbackPrompts=”. Assign one of the following values: • 1:P-Conference header should contain true for “FeedbackPrompts =” • 0: P-Conference header should contain false for “FeedbackPrompts =”.

Protocol-specific parameters

SIP

Parameter	Type	Default value	Description
SUBSCRIBE_SECURITY	Integer	2	Specifies the use of SIP and SIPS subscriptions. Applicable values are between 0 to 2. **Note:** For IP Office, the applicable values are between 0 to 1.
ENABLE_AVAYA_ENVIRONMENT	Integer	1	Specifies the SIP operational mode. Assign one of the following values: • 0: Operates in a mode to comply with the third-party standard SIP proxy provisioning which includes 19 features. • 1: Operates in Avaya environment mode provisioning SIP and AST features and using PPM to download, back up, and restore operations. **Note:** This parameter is only supported in an Avaya Aura® environment. For IP Office, the default value is set to 0.
DISCOVER_AVAYA_ENVIRONMENT	Integer	1	Specifies whether the device discovers that it is in an Avaya environment where SIP AST features are supported. Assign one of the following values: • 0: Do not auto discover AST support. • 1: Auto discover AST support. The SIP proxy server might not support AST. **Note:** This parameter is only supported in an Avaya Aura® environment. For IP Office, the default value is set to 0.
CONFIG_SERVER_SECURE_MODE	Integer	1	Specifies the communication mode for configuration server, that is, whether secure communication through HTTPS is required to access the configuration server. Assign one of the following values: • 0: Use HTTP. • 1: Use HTTPS.

Table continues…

Parameter	Type	Default value	Description
			• 2: Use HTTPS if the SIP transport type is TLS, otherwise use HTTP.
ENABLE_EARLY_MEDIA	Integer	1	Specifies whether to enable early media. Assign one of the following values: • 0: Disabled • 1: Enabled
RDS_INITIAL_RETRY_ATTEMPTS	Integer	15	Specifies Remote Data Source initial retry attempts. The value indicates the number of times the PPM adaptor tries to download from PPM before giving up the PPM server connection. The range is from 1 to 30.
RDS_INITIAL_RETRY_TIME	Integer	2	Specifies Remote Data Source initial retry time. The value indicates the initial delay for a retry for connecting to the PPM server. The range is 2 to 60 seconds.
RDS_MAX_RETRY_TIME	Integer	600	Specifies Remote Data Source maximum retry time. The value indicates the maximum delay interval before giving up on connecting to the PPM server. The range is 2 to 3600 seconds.
OUTBOUND_SUBSCRIPTION_REQUEST_DURATION	Integer	86400	Specifies outbound subscription request duration. The range is from 60 to 31536000 seconds.
USE_QUAD_ZEROES_FOR_HOLD	Integer	0	Specifies the use of quad zeros to signal Hold operation in SDP. Assign one of the following values: • 0: Use “a= directional attributes”. • 1: Use quad zeros.
WAIT_FOR_UNREGISTRATION_TIMER	Integer	32	Specifies the time for which the deskphone waits for before declaring un-registration to be complete. The range is from 4 to 3600.
WAIT_FOR_REGISTRATION_TIMER	Integer	32	Specifies the time for which the deskphone waits for a register response message. If no message is received, registration is retried. The range is from 32 to 3600 seconds.
CONTROLLER_SEARCH_INTERVAL	Integer	16	Specifies the time that the device waits to complete the maintenance check for monitored controllers. The range is from 4 to 3600 seconds.
ASTCONFIRMATION	Integer	60	Specifies the time that the device waits to validate an active subscription when it SUBSCRIBEs to the "avaya-cm-feature-status" package. The range is from 16 to 3600 seconds.

Table continues…

Parameter	Type	Default value	Description
			Note: This parameter is only supported in an Avaya Aura® environment.
ENABLE_OOD_MSG_TLS_ONLY	Integer	1	Specifies whether a received Out-Of-Dialog (OOD) REFER must have TLS transport. Assign one of the following values: • 0: The OOD REFER must have TCP or TLS transport to be auctioned. • 1: The OOD REFER must have TLS transport to be auctioned.

TCP

Parameter	Type	Default value	Description
TCP_KEEP_ALIVE_TIME	Integer	60	Specifies the TCP Keep Alive timer. This time interval is the time for which the deskphone waits before sending out TCP keep-alive message to the far-end. The range is from 10 to 3600 seconds.
TCP_KEEP_ALIVE_INTERVAL	Integer	10	Specifies the TCP keep-alive packet re-transmission interval. After this time interval TCP keep-alive packets are re-transmitted. The range is from 5 to 60 seconds.
TCP_KEEP_ALIVE_STATUS	Integer	1	Specifies the TCP keep alive status. Assign one of the following values: • 0: TCP keep alive disabled. • 1: TCP keep alive enabled.
CONNECTION_REUSE	Integer	1	Specifies whether the device uses two TCP/TLS connection, for both outbound and inbound, or one TCP/TLS connection. Assign one of the following values: • 0: Disable. The device opens an oubound connection to the SIP Proxy and listens to the socket for inbound connection from SIP proxy in parallel. • 1: Enable. The deskphone opens open a connection to the SIP proxy. The device does not listen to inbound connections from SIP proxies, that is, there is only one socket which is used for inbound and outbound.

RTP and RTCP

Parameter	Type	Default value	Description
RTCPCONT	Integer	1	Specifies whether to enable or disable RTCP for audio and video streams between the deskphone and peer. Assign one of the following values: • 0: Disable RTCP. • 1: Enable RTCP.
DTMF_PAYLOAD_TYPE	Integer	120	Specifies the DTMF Payload type. The value from this parameter is used when media offer is sent to the far-end in an INVITE . The range is from 96 to 127.
G726_PAYLOAD_TYPE	Integer	110	Specifies the G.726 Payload type. The value from this parameter is used when media offer is sent to the far-end in an INVITE . The range is from 96 to 127.
SYMMETRIC_RTP	Integer	1	Specifies whether to enforce RTP on the same port. Assign one of the following values: • 0: The device shall accept incoming packets regardless of the UDP source port • 1: The device shall only accept incoming packets if the source port of the incoming UDP datagram matches the destination port used in the UDP datagrams destined for the far-end endpoint. Incoming UDP datagrams that do not satisfy this criterion are discarded.
PLAY_TONE_UNTIL_RTP	Numeric	1	Specifies whether locally-generated ring back tone will stop as soon as SDP is received for an early media session, or whether it will continue until RTP is actually received from the far-end party. Assign one of the following values: • 0: Stop ring back as soon as SDP is received. • 1: Continue ring back tone until RTP is received.

SRTP

Parameter	Type	Default value	Description
MEDIAENCRYPTION	String	9	Specifies the cryptosuite and session parameters for media encryption. You can assign maximum of three comma-separated values from the following list: • 1: aescm128-hmac80. • 2: aescm128-hmac32.

Table continues…

Parameter	Type	Default value	Description
			• 3: aescm128-hmac80-unauth. • 4: aescm128-hmac32-unauth. • 5: aescm128-hmac80-unenc. • 6: aescm128-hmac32-unenc. • 7: aescm128-hmac80-unenc-unauth. • 8: aescm128-hmac32-unenc-unauth. • 9: None. • 10: aescm256-hmac80. • 11: aescm256-hmac32.
SDPCAPNEG	Integer	1	Specifies the SDP capability negotiation. Assign one of the following values: • 0: Disables SDP capability negotiation. • 1: Enables SDP capability negotiation.
ENFORCE_SIPS_URI	Integer	1	Specifies the enforcement of SIPS URI with SRTP. Assign one of the following values: • 0: Not enforced • 1: Enforced
100REL_SUPPORT	Integer	1	Specifies whether the 100rel option tag is included in the INVITE header field per RFC 3262. Assign one of the following values: • 0: The tag is not included. • 1: The tag is included.

Trusted certificates and SCEP

The parameters mentioned below are not present in the auto-generated settings file for IP Office environment.

Parameter	Type	Default value	Description
TRUSTCERTS	String	Null	Specifies the file names of certificates to be used for authentication.
MYCERTURL	String	Null	Specifies the URL to access Simple Certificate Enrollment Protocol (SCEP) server. The device attempts to contact the server only if this parameter is set to other than its default value.

Table continues…

Parameter	Type	Default value	Description
MYCERTCN	String	$SERIALNO	Specifies the Common name (CN) for SUBJECT in SCEP certificate request. The values can either be $SERIALNO or $MACADDR. If the value includes the string "$SERIALNO", that string will be replaced by the phones serial number. If the value includes the string "$MACADDR", that string will be replaced by the phones MAC address.
MYCERTDN	String	Null	Specifies common part of SUBJECT in SCEP certificate request. This value defines the part of SUBJECT in a certificate request including Organizational Unit, Organization, Location, State, and Country that is common for requests from different devices.
MYCERTKEYLEN	Integer	2048	Specifies the private key length in bits to be created in the device for a certificate enrollment. The range is from 1024 to 2048.
MYCERTRENEW	Integer	90	Specifies the percentage used to calculate the renewal time interval out of the device certificate's Validity Object. If the renewal time interval has elapsed the phone starts to periodically contact the SCEP server again to renew the certificate. The range is from 1 to 99.
MYCERTWAIT	Integer	1	Specifies the behavior of the device when performing certificate enrolment. assign one of the following values: • 0: Periodical check in the background. • 1: Wait until a certificate or a denial is received or a pending notification is received.
MYCERTCAID	String	CAIdentifier	Specifies the Certificate Authority Identifier. Certificate Authority servers may require a specific CA Identifier string in order to accept GetCA requests. If the device works with such a Certificate Authority, the CA identifier string can be set through this parameter.
SCEPPASSWORD	String	$SERIALNO	Specifies a challenge password to use with SCEP. The value of SCEPPASSWORD, if non-null, is included in a challengePassword attribute in SCEP certificate signing requests. If the value contains $SERIALNO, $SERIALNO is replaced by the value of SERIALNO,. If the value contains $MACADDR, $MACADDR is replaced by

Table continues…

Parameter	Type	Default value	Description
			the value of MACADDR without the colon separators.

TLS

Parameter	Type	Default value	Description
TLSSRVRID	Integer	1	Specifies whether the TLS server identification is required. Assign one of the following values: • 0: No certificate match necessary. TLS connection will be established. • 1: Certificate match required. TLS connection will only be established if the server's identity matches the server's certificate.

LLDP

Parameter	Type	Default value	Description
LLDP_ENABLED	Integer	2	Specifies whether to enable LLDP. Assign one of the following values: • 0: Disabled. • 1: Enabled. • 2: Enabled, but only begin transmitting if an LLDP frame is received.

Dial plan parameters

Parameter	Type	Default value	Description
DIALPLAN	String	Null	Specifies one or more valid dial strings. The range is 0 to 1023 characters.
PHNCC	String	1	Specifies the dial plan country code.
PHNDPLENGTH	Numeric	5	Specifies the dial plan internal extension length. The range is from 3 to 13.
PHNIC	String	011	Specifies the dial plan international access code.
PHNLD	String	1	Specifies the dial plan long distance access code.
PHNLDLENGTH	Numeric	10	Specifies the dial plan national telephone number length. The range is from 5 to 15.

Table continues…

Parameter	Type	Default value	Description
PHNOL	String	9	Specifies the dial plan public network access code.
PHNEMERGNUM	String	Null	Specifies the emergency number.
ENABLE_REMOVE_PSTN_ACCESS_PREFIX	Numeric	0	Specifies whether to enable the removal of the PSTN access prefix. Assign 0 or 1. **Note:** This parameter is only supported in an Avaya Aura® environment.
LOCAL_DIAL_AREA_CODE	Numeric	0	Specifies whether the user must dial area conde for calls within same area code. Assign 0 or 1.
PHNLAC	String	Null	Specifies the local area code.
PHNMOREEMERGNUMS	String	Null	Specifies the list of additional emergency numbers. The range is from 0 to 100.

Video parameters

Parameter	Type	Default value	Description
ENABLE_VIDEO	Integer	1	Specifies whether to enable video. Assign one of the following values: • 0: Disables video. • 1: Enables video.
VIDEO_PAYLOAD_LENGTH	Integer	0	Specifies the video packets payload length. Specify a value in the range of to 1200 to 1460 or 0 for automatic.
ENABLE_FIR	Integer	1	Specifies whether key frame requests are supported using RTCP Full Intra Requests (FIR) according to RFC 5104. Assign one of the following values: • 0: RTCP FIR is not SDP negotiated with remote peer. • 1: RTCP FIR is SDP negotiated with remote peer. RTCP FIR messages are generated and received only if both peers support RTCP FIR.
ENABLE_PLI	Integer	1	Specifies whether key frame requests are supported using RTCP Picture Loss Indication (PLI) according to RFC 4585). Assign one of the following values: • 0: RTCP PLI is not SDP negotiated with remote peer.

Table continues…

Parameter	Type	Default value	Description
			• 1: RTCP PLI is SDP negotiated with remote peer (default). TCP PLI messages are generated and received only if both peers support RTCP PLI.
ENABLE_TMMBR	Integer	1	Sspecifies whether Temporary Maximum Media Stream Bit Rate Requests (TMMBR) RTCP requests, according to RFC 5104, are sent to remote peer for bit rate adaptation and whether the device responds to TMMBR RTCP requests received. Assign one of the following values: • 0: RTCP TMMBR is not SDP negotiated with remote peer. • 1: RTCP TMMBR is SDP negotiated with remote peer. RTCP TMMBR messages are generated and received only if both peers support RTCP TMMBR..
VIDEO_MAX_RX_RESOLUTION	Integer	6	Specifies the maximum video resolution that the device requests from the other side. Assign one of the following values: • 4: 480p • 5: 720p • 6: 1080p
VIDEO_MAX_TX_RESOLUTION	Integer	6	Specifies the maximum video resolution that the device encodes and sends. Assign one of the following values: • 1: 180p • 2: 240p • 3: 360p • 4: 480p • 5: 720p • 6: 1080p
VIDEO_MAX_RX_BANDWIDTH	Integer	4300	Specifies a limit for an overall SDP requested bandwidth consumed by RTP for video including IP and UDP overheads, but not Ethernet. The range is from 80 to 4300.
VIDEO_MAX_TX_BANDWIDTH	Integer	2500	Specifies the limit for an overall bandwidth consumed by transmitted RTP for video including IP and UDP overheads, but not Ethernet. The maximum limit allows 4096 raw H.264 bandwidth. The range is from 80 to 4300.

Table continues…

Parameter	Type	Default value	Description
DYNAMIC_VIDEO_SIZE_REQUEST_DELAY	Integer	20	Specifies the amount of time in seconds for which the device waits before asking the remote party to reduce the resolution to match a newly selected video window size. The range is from 1 to 600.
DYNAMIC_VIDEO_SIZE_REQUEST	Integer	1	Specifies whether the device notifies the other device about the changed size of the video window so that the other device can change the transmitted video accordingly. Assign one of the following values: • 0: Disabled. • 1: TMMBR.
VIDEO_H264_PROFILE	Integer	100	Specifies the maximal profile level that the system can use. Set the value to 66, which implies a baseline profile, or 100, which implies both high and baseline profile.
PINHOLE_KEEPALIVE_INTERVAL	Integer	15	Specifies the maximal time between consecutive video RTP packets. The range is from 15 to 60 seconds or 0 for no RTP keepalives.
VIDEO_CALL_DISPLAY_MODE	Integer	1	Specifies the default display mode for a video call. Assign one of the following values: • 0: Internal built-in screen. • 1: External screen if connected. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
CLONE_DISPLAY	Integer	0	Specifies the display cloning behavior of the Collaboration Station when an external monitor and a personal computer is connected to it through the two HDMI ports. Assign one of the following values: • 0: - During an active video call: Supports picture in picture (PiP) for the active video call. The personal computer screen is displayed on the external monitor and the video call container is overlaid. - When there is no active video call: Only the personal computer screen is displayed on the external monitor.

Table continues…

Parameter	Type	Default value	Description
			• 1: Displays only the Collaboration Station screen on the external monitor. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.

Audio parameters

Name	Description
Received Coding	G.711, G.722, G.726A, or G.729
Packet Loss	Missing, late, and out-of-sequence packets are counted as lost if they are discarded. Packets are not counted as lost until a subsequent packet is received and the loss confirmed by the RTP sequence number.
Packetization Delay	The amount of audio data in each RTP
One-way Network Delay	The number is half the value that RTCP or SRTCP computes for the round-trip delay to the device where the RTP is transmitted. For the calls that have a large geographic distance this number is expected to be larger than for local calls.
Network Jitter Delay	The average delay introduced by the jitter buffer on the deskphone.

Logging and debugging parameters

Parameter	Type	Default value	Description
SYSLOG_ENABLED	Integer	0	Specifies whether the sys log notification is enabled. Assign one of the following values: • 0: Syslog off. • 1: Syslog on.
SYSLOG_LEVEL	Integer	3	Specifies the severity level. The device sends a syslog message if an event occurs with a severity

Table continues…

Parameter	Type	Default value	Description
			level equal or less than the value specified in this parameter. Assign one of the following values: • 3: Error • 4: Warning • 5: Notice • 6: Informational • 7: Debug
LOCAL_LOGS_ENABLED	Integer	1	Specifies whether the local storage of log messages is enabled. Assign one of the following values: • 0: Local log off • 1: Local log on
LOCAL_LOG_LEVEL	Integer	4	Specifies the severity level for storing event logs locally. The device stores entries to a local event log when an event occurs with a severity level equal or less than the value specified in this parameter. Assign one of the following values: • 3: Error • 4: Warning • 5: Notice • 6: Informational • 7: Debug • 8: Stream debug
LOG_CATEGORY	String	All	Specifies a comma-separated list of keywords in standard string format for logging categories. Logging implementation blocks all traces at the Warning or lower severity level unless the category corresponding to a given trace is enabled. The device filters all ANDROID and KERNEL syslog or log categories if you do not configure this parameter for these categories or if the value of the parameter is not set to All. If the log level is set to Warning or a lower level, this parameter enables low-level traces from adaptors or manager as indicated. This parameter applies to both syslog and local logging mechanisms. The supported categories are :ALL, ANDROID, 8021X, ADAPMGR, ALSIP, AST, AUDIO, CALENDAR, CCMP, CCSPROFILE, CERTMGMT,

Table continues…

Parameter	Type	Default value	Description
			CONFERENCE, CONFIG, CONFIG_MULTI, CONTACT, CORE, DATETIME, DAVDATA, DEVICE, DHCP, DIAL, EEPROMDATA, ENCRYPT, EXTAPP, FAILOVER, FAVORITE, HISTORY, HTTP, KERNEL, LLDP, LOCALDATA, MEDIA, MEDIAAUDIOCODING, MEDIAAUDIODEVICE, MEDIAAUDIOMIXERCLIENT, MEDIAAUDIOMIXERSERVER, MEDIAAUDIOPROCESSING, MEDIAFILE, MEDIARTPRTCP, MEDIASRTP, MEDIATRANSPORT, MEDIAUTILITY, MEDIAVIDEO, MEDIAVIDEOCAPTURE, MEDIAVIDEOCODING, MEDIAVIDEOMIXER, MEDIAVIDEOPROC, MEDIAVIDEORENDERER, MSGMGR, MSG_ROUTING, MSM, MWI, NETADAP, NETMGR, ONEXPAUCDATA, PERSLABELS, PLATFORM_COMP, PPMDATA, PPMMESSAGE, POWER, PRESENCE, QOS, REG, SCRIPT, SCRIPTDATA, SECURITY, SESSION, SESSION_VIDEO, SHARED_CNTRL, SIGADAP, SIGNAL, SIGNAL_VIDEO, SIGNALING_COMP, SIPEVENTS, SIPMESSAGE, SM, SSHDADAP, SUBSCRIBE, THREADWDOG, UI, UPGRADE, VIDEO, VMM, and WEB.
SSH_ALLOWED	Integer	0	Specifies whether and how Secure Shell (SSH) is supported. Assign one of the following values: • 0: Disabled. • 1: Enabled with challenge/response authentication.
SSH_BANNER_FILE	String	Null	Specifies the file name or URL of a file that contains warning banner text that is sent to SSH clients before authentication.
SSH_IDLE_TIMEOUT	Integer	10	Specifies the number of minutes of bidirectional inactivity after which an SSH connection is terminated. The range is from 0 to 32767. Assign one of the following values: • 0: No timeout. • 1–32767: Number of minutes of inactivity after which SSH is disabled.
ENABLE_RECORDING	Integer	0	Specifies whether audio debug recording is enabled. Assign one of the following values: • 0: Disabled • 1: Enabled

Upgrade related parameters

Upgrade related parameters

Upgrade related parameters

Parameter	Type	Default value	Description
UPGRADE_POLLING_PERIOD	Integer	60	Specifies the polling interval in minutes between polling both firmware and settings file. The range is from 0 to 10080. Assign one of the following values: • 0: Disabled • 1–10080: Enabled
UPGRADE_DLOAD_START	String	Null	Specifies the start time at which phone tries to download the firmware file. The format is Dddhh. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
UPGRADE_DLOAD_END	String	Null	Specifies the end time at which phone stop tries to download new firmware file. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
UPGRADE_INSTALL_DATE_TIME	String	1970-01-01T00:00	Specifies the date and time after which new firmware and settings file are installed.
UPGRADE_POLICY	Integer	2	Specifies whether the firmware and settings files update is done after reset only, reset and policy configuration parameters, or policy only. Assign one of the following values: • 0: Update of firmware and settings files after reset only. • 1: Update of firmware and settings files according to the policy rules. Reset does not trigger new update of firmware and settings files. • 2: Update upgrade/settings files and firmware after any reset and policy rules.

Table continues…

Parameter	Type	Default value	Description
DLOAD_RND_AFTER_RESET	Integer	0	Specifies the interval in seconds over which downloading attempts is randomized after reboot. Assign one of the following values: • 0: No randomization. • 1–32767: Randomization.
DLOAD_RND	Integer	3600	Specifies the interval in seconds over which downloading attempts is randomized during background downloads. Assign one of the following values: • 0: No randomization. • 1–32767: Randomization.

Configuration parameters

Generic functionality

Parameter	Type	Default value	Description
ENABLE_PRESENCE	Integer	1	Specifies whether the presence function is enabled. Assign one of the following values: • 0: Disabled • 1: Enabled **Note:** This parameter is supported only in an Avaya Aura® environment.
ENABLE_APPS	String	Null	Specifies the embedded applications list separated by commas to be available on the device.
DEFAULT_SEARCH_DIRECTORY	Integer	1	Specifies the directory to be parsed while searching contacts on the device. Assign one of the following values: • 1: Aura • 2: Exchange
ENABLE_ONLINE_SEARCH	Integer	1	Specifies whether or not the default contact search directory is to be parsed. Assign one of the following values: • 0: Disabled • 1: Enabled

Table continues…

Parameter	Type	Default value	Description
SIMULTANEOUS_REGISTRATIONS	Integer	3	Specifies the number of Session Managers for simultaneous registration with the phone. The range is from 1 to 3. **Note:** The default value for an IP Office environment is set to 1.
ENABLE_PPM_SOURCED_SIPPROXYSRVR	Integer	1	Specifies the source of the SIP proxy server information as PPM. The range is from 0 to 1. **Note:** The default value for an IP Office environment is set to 0.
ENABLE_G711A	Integer	1	Specifies whether G.711A codec capability of phone is enabled. Assign one of the following values: • 0: Disabled • 1: Enabled
ENABLE_G711U	Integer	1	Specifies whether G.711U codec capability of phone is enabled. Assign one of the following values: • 0: Disabled • 1: Enabled
ENABLE_G729	Integer	1	Specifies whether G.729(A) codec capability of phone is enabled. Assign one of the following values: • 0: G.729 disabled. • 1: G.729(A) enabled, without Annex B support. • 2: G.729(A) enabled with Annex B support.
ENABLE_G722	Integer	1	Specifies whether G.722 codec of phone is enabled. Assign one of the following values: • 0: Disabled • 1: Enabled
ENABLE_G726	Integer	1	Specifies whether G.726 capability of phone is enabled. Assign one of the following values: • 0: Disabled • 1: Enabled **Note:** The default value for an IP Office environment is set to 0.

Table continues…

Parameter	Type	Default value	Description
BRANDING_VOLUME	Integer	5	Specifies the level of the Avaya audio brand. Assign one of the following values: • 1: 12 db below nominal • 2: 9 db below nominal • 3: 6 db below nominal • 4: 3 db below nominal • 5: nominal • 6: 3 db above nominal • 7: 6 db above nominal • 8: 9 db above nominal

Deskphone-specific parameters

These parameters can be used as testable configuration parameters with the IF command as follows.

IF $MODEL4 SEQ H175 GOTO H175CFG

Parameter	Type	Default value	Description
MACADDR	AUTH	Factory setting	Specifies the MAC address of the telephone.
MODEL4	String	Factory setting	Specifies the name of the telephone model . The range is four ASCII characters.
GROUP	Integer	0	Specifies a group identifier to allow to download during start-up a specific configuration set for a dedicated user group . The range is from 0 to 999.
MODEL	String	1	Specifies the model identifier of the telephone. The range is from 8 to 10 characters.

Configuration parameter download

Parameter	Type	Default value	Description
AUTH	Integer	0	Specifies the authentication flag for all files download. Assign of the following values: • 0: Secure files download is not required. • 1: Secure files download is required.

Android configuration parameter

Parameter	Type	Default value	Description
KEY_LAYOUT_FILES	String	Null	Specifies the absolute or relative URL for downloading the key layout files.

Port ranges parameters

Port ranges parameters

Parameter	Type	Default value	Description
RTP_PORT_LOW	Integer	5004	Specifies the lower limit of a port range to be used by RTP, RTCP, SRTP, or SRTCP connections when the parameter CONNECTION_REUSE is set to 0. The range is from 1024 to 65503.
RTP_PORT_RANGE	Integer	40	Specifies the width of port range to be used by used by RTP, RTCP, SRTP, or SRTCP connections when the parameter CONNECTION_REUSE is set to 0. The range is from 32 to 64511.
SIG_PORT_LOW	Integer	1024	Specifies the lower limit of a port range to be used for SIP signaling independent, if TCP or TLS over TCP. The range is from 1024 to 65503.
SIG_PORT_RANGE	Integer	64511	Specifies the width of port range to be used for SIP signaling independent, if TCP or TLS over TCP. The range is from 32 to 64511.

Audio operation and quality monitoring

Audio operation and quality monitoring

Parameter	Type	Default value	Description
QLEVEL_MIN	1 ASCII numeric digit	4	Specifies the minimum quality level for which a low local network quality is not displayed. Assign one of the following values: • 1: Never display icon. • 2: Packet loss is > 5% or round trip network delay is > 720 ms or jitter compensation delay is > 160 ms.

Table continues…

Parameter	Type	Default value	Description
			• 3: Packet loss is > 4% or round trip network delay is > 640 ms or jitter compensation delay is > 140 ms. • 4: Packet loss is > 3% or round trip network delay is > 560 ms or jitter compensation delay is > 120 ms. • 5: Packet loss is > 2% or round trip network delay is > 480 ms or jitter compensation delay is > 100 ms. • 6: Packet loss is > 1% or round trip network delay is > 400 ms or jitter compensation delay is > 80 ms. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
WBCSTAT	1 ASCII numeric digit	1	Specifies whether a wideband codec indication is displayed when used. Assign one of the following values: • 0: Wideband codec indication is not displayed. • 1: Wideband codec indication is displayed.

General and phone application timer

General and phone application timer

Parameter	Type	Default value	Description
REGISTERWAIT	Integer	900	Specifies the interval in seconds for next reregistration to SIP server. The range is 30 to 86400.
NO_DIGITS_TIMEOUT	Integer	20	Specifies the duration for timeout when no digit is entered. The range is from 1 to 60.
INTER_DIGIT_TIMEOUT	Integer	5	Specifies the duration for timeout between entered digits. The range is from 1 to 10.
FAILED_SESSION_REMOVAL_TIMER	Integer	30	Specifies the timer to remove failed call session. The range is from 5 to 999.

Table continues…

Parameter	Type	Default value	Description
FAST_RESPONSE_TIMEOUT	Integer	4	Specifies the fast response timer. The range is from 0 to 32.
RECOVERYREGISTERWAIT	Integer	60	Specifies the interval for reactive monitoring. The range is from 10 to 36000.
FAILBACK_POLICY	String	auto	Specifies the fail back policy. Assign one of the following values: • admin • auto
WAIT_FOR_INVITE_RESPONSE_TIMEOUT	Integer	60	Specifies the maximum duration in seconds that the phone waits to get a response after receiving 100 trying. The range is 30 to 180 seconds.

Deskphone interface settings parameters

Common operation

Parameter	Type	Default value	Description
BAKLIGHTOFF	Integer	120	Specifies the idle time in minutes after which the device turns off the backlight. The range is from 0 to 999. **Note:** The parameter is only applicable for the registered devices that are currently logged-in.
RINGTONESTYLE	Integer	0	Specifies the style of classic ringtone that the device offers. Assign one of the following values: • 0: For North American ringtones. • 1: For European ringtones.
AUDASYS	Integer	3	Specifies whether the user can set the audible alerting to the lowest level or to zero. Assign one of the following values: • 0: To set the audible alerting to the lowest audible setting. • 1: To set the audible alerting to zero. • 2: To set the audible alerting to the lowest audible setting.

Table continues…

Parameter	Type	Default value	Description
			• 3: To set the audible alerting to zero.
PHNNUMOFSA	Integer	3	Specifies the number of session appearances that the device supports while operating in a non-Avaya environment. The range is from 1 to 10.
ENHDIALSTAT	Integer	1	Specifies the enhanced local dialing status. Assign one of the following values: • 0: Disables the feature. • 1: Partially enables the feature, that is, the dialing rules do not apply for dialing from Contacts. • 2: Fully enables the feature, that is, the dialing rules also apply for dialing from Contacts.
SEND_DTMF_TYPE	Integer	2	Specifies whether the DTMF tones are send as in-band or out-band. Assign one of the following values: • 1: Send as in-band, that is, as regular audio. • 2: Send as out-band, that is, negotiation and transmission of DTMF occurs according to RFC 2833. If the far end does not support RFC 2833, send as in-band DTMF tones.
INGRESS_DTMF_VOL_LEVEL	Integer	–12	Specifies the power level of the tone in dBm0 after dropping the sign. The range is from –20 to –7.
SIPCONFERENCECONTINUE	Integer	0	Specifies whether to stop or continue the conference when the host is dropped from the conference. Assign one of the following values: • 0: Conference stops. • 1: Conference continues by transferring the host to the second party. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.

Audio settings

Parameter	Type	Default value	Description
AGCHAND	Integer	0	Specifies the status of Automatic Gain Control (AGC) for handset. Assign one of the following values: • 0: AGC off

Table continues…

Parameter	Type	Default value	Description
			• 1: AGC on
AGCHEAD	Integer	0	Specifies the status of Automatic Gain Control (AGC) for a headset. Assign one of the following values: • 0: AGC off • 1: AGC on
AGCSPKR	Integer	0	Specifies the status of Automatic Gain Control (AGC) for the speaker. Assign one of the following values: • 0: AGC off • 1: AGC on
REDIRECT_TONE	Integer	1	Specifies the single beep of call coverage tone played when at least one of the provisional responses is a 181 Call Forwarded and no RTP packets are received. The range is from 1 to 4.
RINGTONES	String	Null	Specifies the list of audio files to be downloaded as ring tones and offered to the user for selection. The range is from 0 to 1023 octets of UTF-8 characters.
HEADSET_PROFILE_DEFAULT	Integer	1	Specifies the number of the default headset audio profile. The range is from 1 to 20.
HEADSET_PROFILE_NAMES	String	Null	Specifies the names to be displayed for headset audio profile selection. The range is from 0 to 255 octets of UTF-8 characters.
AUDIOSTHS	Integer	0	Specifies the settings for the handset sidetone. Assign one of the following values: • 0: Normal. • 1: Three level softer than normal. • 2: Off. • 3: One level softer than normal. • 4: Two levels softer than normal. • 5: Four levels softer than normal. • 6: Five levels softer than normal. • 7: Six levels softer than normal. • 8: One level louder than normal. • 9: Two levels louder than normal. **Note:** This parameter is not present in the auto-generated settings file for IP Office

Table continues…

Parameter	Type	Default value	Description
			environment. You can provision it through a custom settings file on a different file server.
AUDIOSTHD	Integer	0	Specifies the settings for the headset sidetone. Assign one of the following values: • 0: Normal. • 1: Three level softer than normal. • 2: Off. • 3: One level softer than normal. • 4: Two levels softer than normal. • 5: Four levels softer than normal. • 6: Five levels softer than normal. • 7: Six levels softer than normal. • 8: One level louder than normal. • 9: Two levels louder than normal. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.

Display settings

Parameter	Type	Default value	Description
LOCALLY_ENFORCE_PRIVACY_HEADER	Integer	0	Specifies that the display is locally enforced when a Privacy header is included in the INVITE for an incoming call. Assign one of the following values: • 0: Disabled. The responsibility for privacy is with the CM/SM, the endpoint displays any CallerId received in the From or Contact headers as done for a normal, non-private call. • 1: Enabled. The responsibility for privacy is with the endpoint, the endpoint displays the localized string as Restricted.
ENFORCE_DVI	Integer	1	Specifies whether the Digital Visual Interface (DVI) is enforced when the PC display is pass through the phone. Assign one of the following values: • 0: DVI is not enforced. Screen resolution is 720p.

Table continues…

Parameter	Type	Default value	Description
			• 1: DVI is enforced. Screen resolution is 1080p using DVI. HDMI is not supported. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
LOGOS	String	Null	Specifies the list of custom logo definitions for the background display. Each logo tuple contains a label and a full URL. **Note:** • Change in the parameter label does not trigger update for all the files. However, change in the URL filename triggers deletion of that file. • This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
CURRENT_LOGO	String	Null	Specifies the selected background logo for display. The string is empty for the default logo. It is recommended to use the background image of at least 1440 x 800 resolution. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
LOGOSTAT	Integer	1	Specifies whether the wallpaper configuration is done by user or administrator. Assign one of the following values: • 0: Administrator configured. • 1: User configured. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.

Table continues…

Parameter	Type	Default value	Description
SCREENSAVERURL	String	Null	Specifies the URL of the background for screen saver. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
LOCKSCREENURL	String	Null	Specifies the URL of the background for the Lock screen. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
HOME_SCREEN_GRID_SIZE	Integer	1	Specifies the grid size of the icon on the Home screen. Assign one of the following values: • 1: 6 x 3 icons (width x height) • 2: 4 x 2 icons (width x height)
ADMIN_INITIAL_SCREEN	String	PHONE	Specifies the screen that is presented to the user in the following scenarios: • When the user logs in to the device. • When the user initiates a call/conference and then immediately disconnects. • When the user is active on more than one call and all active calls are disconnected. Assign one of the following values: • PHONE • HOMESCREEN **Note:** If an application is active on the phone, the user returns to the application after the call is cancelled or ended. For example, if the user has a browser application active, he returns to the browser and not to the screen specified by this parameter.

Table continues…

Parameter	Type	Default value	Description
EXTENSION_ON_TOP_LINE	Integer	1	Specifies the device to display device extension number on the Top bar. Assign one of the following values: • 1: Hides the device extension number on the Top bar. • 2: Displays the device extension number on the Top bar.

Language and country settings

Parameter	Type	Default value	Description
ISO_SYSTEM_LANGUAGE	String	en-US	Specifies the locale which controls: • Language presented to the user. • Date, time, and numbers format for the relevant locale. Assign one of the following values: • en_CA • en_IN • en_NZ • en_SG • en_GB • en_US • fr_BE • fr_CA • fr_FR • fr_CH • ru_RU • pt_BR • zh_CN • ja_JP • ko_KR • ar_EG • iw_IL • es_US

Table continues…

Parameter	Type	Default value	Description
			Note: Reboot the phone after you change the system language.
COUNTRY	String	Undefined	Specifies the country of operation for specific dial tone generation, Wi-Fi, DECT, and the default anti flickering frequency for camera – 50 Hz or 60 Hz.

Network parameters

General network parameters

Parameter	Type	Default value	Description
DHCPSTD	Integer	0	Specifies the DHCP lease violation flag. Assign one of the following values: • 1: Comply with the DHCP standard, that is, (immediately release IP address, if DHCP lease expires. • 0: Enter proprietary state, that is, continue to use IP address, if DHCP lease expires.
ICMPDU	Integer	1	Specifies whether the ICMP Destination Unreachable messages are generated. Assign one of the following values: • 0: Destination Unreachable messages will not be transmitted. • 1: Destination Unreachable messages will only be transmitted for the UDP port in the range of 33,434 to 33,523. • 2: Destination Unreachable messages will be transmitted.
ICMPRED	Integer	0	Specifies whether the ICMP redirect messages will be processed. Assign one of the following values: • 0: Received Redirect messages will not be processed. • 1: Received Redirect messages will be processed per RFC 1122.

Table continues…

Parameter	Type	Default value	Description
MTU_SIZE	Integer	1500	Specifies the Maximum Transmission Unit size for Ethernet interface only and not for Wi-Fi. Assign one of the following values: • 1496 • 1500
REUSETIME	Integer	60	Specifies the IP address reuse timeout for Ethernet interface only and not for Wi-Fi. The range is from 0 to 20,999.
DECTSTAT	Integer	1	Specifies whether the DECT menu option in the Setting app is enabled for the user. Assign one of the following values: • 0: The DECT and menu option is disabled in the Settings app and the user cannot change it. • 1: The DECT and menu option is enabled in the Settings app and the user can change it to enable or disable the wireless handset.
BLUETOOTHSTAT	Integer	1	Specifies whether Bluetooth is allowed for user configuration. Assign one of the following values: • 0: The Bluetooth and menu option is disabled in the Settings app and the user cannot change it. • 1: The Bluetooth and menu option is enabled in the Settings app and the user can change it to enable or disable Bluetooth.
WIFISTAT	Integer	0	Specifies whether Wi-Fi is allowed for user configuration. Assign one of the following values: • 0: The Wi-Fi and menu option is disabled in the Settings app and the user cannot change it. • 1: The Wi-Fi and menu option is enabled in the Settings app and the user can change it to enable or disable the Wi-Fi.
GRATARP	Integer	0	Specifies whether an existing ARP cache entry is updated with a MAC address received in a gratuitous ARP message. Assign one of the following values: • 0: Gratuitous ARP messages will be ignored. • 1: Gratuitous ARP messages will be processed to update an existing ARP cache entry. **Note:** This parameter is not present in the auto-generated settings file for IP Office

Table continues…

Parameter	Type	Default value	Description
			environment. You can provision it through a custom settings file on a different file server.
IPADD	String	0.0.0.0	Specifies the IP address of the phone. The range is from 7 to 15 ASCII characters. This is a testable parameter. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
CAPTIVE_PORTAL_SERVER	String	Null	Specifies the URL of the captive portal server for HTTP authentication to use the Internet. Use one of the following options for configuration: • [http://]hostname[:port][/path] • [https://]hostname[:port][/path] **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.

Ethernet parameters

Parameter	Type	Default value	Description
PHY1STAT	Numeric	1	Specifies the speed and duplex mode of Ethernet line interface. Assign one of the following values: • 1: Auto negotiation speed and duplex. • 2: 10Mbps half-duplex operation. • 3: 10Mbps full-duplex operation. • 4: 100Mbps half-duplex operation. • 5: 100Mbps full-duplex operation.
PHY2STAT	Numeric	1	Specifies the speed and duplex mode of the secondary Ethernet line interface or disables the

Table continues…

Parameter	Type	Default value	Description
			secondary Ethernet line interface. Assign one of the following values: • 0: Disabled. • 1: Auto negotiation speed and duplex. • 2: 10Mbps half-duplex operation. • 3: 10Mbps full-duplex operation. • 4: 100Mbps half-duplex operation. • 5: 100Mbps full-duplex operation.
PHY2TAGS	Numeric	0	Specifies whether tags are stripped from frames forwarded to PHY2. Assign one of the following values: • 0: Remove tags from frames forwarded to PHY2. • 1: Do not remove tags from frames forwarded to PHY2.
PHY2_AUTOMDIX_ENABLED	Numeric	1	Specifies whether Auto-MDIX is enabled on PHY2. Assign one of the following values: • 0: Auto-MDIX will be disabled on PHY2. • 1: Auto-MDIX will be enabled on PHY2. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
ASSUME_SP_POE	Numeric	0	Specifies whether Single port PoE injector is connected to the device. Assign one of the following values: • 0: Single port PoE injector is not connected to the device. • 1: Single port PoE injector is connected to the device.
SP_POE_POWER	Numeric	20	Specifies how much power is provided when the device is connected to Single port PoE injector. The range is from 16 to 25.

QoS parameters

Parameter	Type	Default value	Description
L2QAUD	Numeric	6	Specifies the layer 2 audio priority value. The range is from 0 to 7. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
L2QVID	Numeric	5	Specifies layer 2 video priority value. The range is from 0 to 7. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
L2QSIG	Numeric	6	Specifies the layer 2 signaling priority value. The range is from 0 to 7. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
DSCPAUD	Numeric	46	Specifies the differentiated Services Code Point for audio. The range is from 0 to 63.
DSCPSIG	Numeric	34	Specifies the differentiated Services Code Point for signaling. The range is from 0 to 63.
DSCPVID	Numeric	34	Specifies the differentiated Services Code Point for video. The range is from 0 to 63.

VLAN parameters

The parameters mentioned below are not present in the auto-generated settings file for IP Office environment.

Parameter	Type	Default value	Description
L2Q	Numeric	0	Specifies 802.1Q tagging mode. Assign one of the following values: • 0: Auto • 1: On • 2: Off
L2QVLAN	Numeric	0	Specifies the 802.1Q VLAN identifier. The range is 0 to 4094.
VLANTEST	Numeric	60	Specifies the timer for DHCPOFFER reception on a non-zero VLAN. The range is 0 to 999.
VLANSEP	Numeric	1	Specifies whether to enables the VLAN separation. Assign one of the following values: • 0: Disabled • 1: Enabled
PHY2VLAN	Numeric	0	Specifies the VLAN ID for tagged frames on the secondary Ethernet Interface. The range is 0 to 4094.

IEEE 802.1.x parameters

The parameters mentioned below are not present in the auto-generated settings file for IP Office environment.

Parameter	Type	Default value	Description
DOT1XSTAT	Numeric	0	Specifies the IEEE 802.1X status for Ethernet interface. Assign one of the following values: • 0: Supplicant operation disabled. • 1: Supplicant operation enabled, but responds only to received unicast EAPOL messages. • 2: Supplicant operation enabled, responds to received unicast and multicast EAPOL messages.
DOT1X	Numeric	0	Specifies the IEEE 802.1X operational mode for Ethernet interface. Assign one of the following values: • 0: PAE multicast pass-through without proxy Logoff. • 1: PAE multicast pass-through with proxy Logoff.

Table continues…

Parameter	Type	Default value	Description
			• 2: No PAE multicast pass-through or proxy Logoff.
DOT1XEAPS	String	MD5	Specifies a list of EAP methods for IEEE 802.1x authentication. For now, the values supported are TLS and MD5.

Account and password parameters

The parameters mentioned below are not present in the auto-generated settings file for IP Office environment.

Parameter	Type	Default value	Description
PROCPSWD	String	27238	Specifies the password to gain administrator rights for local procedures on the device.

Apps parameters

Calendar app

The parameters mentioned below are not present in the auto-generated settings file for IP Office environment.

Parameter	Type	Default value	Description
CALENDAR_PARTICIPANT_CODE_STRING	String	participant;participant code;participant-code;code;pc	Specifies participant code as a list of semicolon separated values. The parameter is used for Avaya Aura® Conferencing.
CALENDAR_HOST_CODE_STRING	String	host;host code;host-code;hc	Specifies host code as a list of semicolon separated values. The parameter is used for Avaya Aura® Conferencing.
CALENDAR_MEETING_ID_STRING	String	meeting;meeting id;meeti	Specifies meeting ID as a list of semicolon separated values. The parameter is used for Avaya Scopia®.

Table continues…

Parameter	Type	Default value	Description
		ng-id;mid;id	
CALENDAR_MEETING_PIN_STRING	String	meeting pin;pin; meeting-pin	Specifies meeting pin as a list of semicolon separated values. The parameter is used for Avaya Scopia®.
CALENDAR_PHONE_NUM_MIN_DIGITS	Integer	4	Specifies the minimal number of digits required for the device to identify a number in the location or body of the message. The range is 4 to 21.

Lock app

Parameter	Type	Default value	Description
ENABLE_PHONE_LOCK	Integer	0	Specifies whether the lock screen password is enabled. Assign one of the following values: • 0: Disables lockout • 1: Enables lockout
PHONE_LOCK_IDLETIME	Integer	60	Specifies the lock screen inactivity timeout. The range is from 1 to 10080 minutes. The idle lock time overrides the value that Microsoft Exchange Server sends if the deskphone is synchronized to an Exchange Server that enforces a security policy for Android devices. **Note:** This parameter is not present in the auto-generated settings file for IP Office environment. You can provision it through a custom settings file on a different file server.
PHONE_LOCK_PASSWORD_FAILED_ATTEMPTS	Integer	8	Specifies the number of failed attempts before the device locks out. The range is from 0 to 20.

Messaging app

Parameter	Type	Default value	Description
MSGNUM	String	Null	Specifies the telephone number for use by the messaging application. **Note:** This parameter is not present in the auto-generated settings file for IP Office

Table continues…

Parameter	Type	Default value	Description
			environment. You can provision it through a custom settings file on a different file server.
PSTN_VM_NUM	String	Null	Specifies the telephone number for use by the messaging application in a non-Avaya or failover server environment.

Presence parameters

The following parameters are supported only in an Avaya Aura® environment.

Parameter	Type	Default value	Description
ENABLE_AUTOMATIC_ON_THE_PHONE_PRESENCE	Integer	1	Specifies whether to activate automatic presence status update when user goes on-hook or off-hook. Assign one of the following values: • 0: Disabled • 1: Enabled
PRESENCE_ACL_CONFIRM	Integer	2	Specifies the handling of Presence ACL updates. When a watcher list is received (presence.winfo NOTIFY) which contains one or more watchers with the pending status, the value of this parameter defines the action taken by the device. Assign one of the following values: • 0: Auto Confirm. When a watcher list is received containing ‘pending’ watchers, the phone will automatically PUBLISH an approval to allow immediate presence monitoring. • 1: Ignore. The device will not take any action on ‘pending’ watchers. • 2: Prompt. Provided to allow future support for the phone directly prompting the user to Allow or Deny the watcher’s request.
AWAY_TIMER_VALUE	Integer	30	Specifies the time for which the device assumes that the user is not away from the device if there was no interaction with the device for more than the time specified. The range is from 1 to 1500 minutes.
AWAY_TIMER	Integer	1	Specifies whether the device can report away state. Assign one of the following values: • 0: Disabled

Table continues…

Parameter	Type	Default value	Description
			• 1: Enabled

Microsoft Exchange parameters

Parameter	Type	Default value	Description
EXCHANGE_SERVER_SECURE_MODE	Integer	1	Specifies whether to use HTTP or HTTPS to contact Microsoft Exchange Server. Assign one of the following values: • 0: Use HTTP. • 1: Use HTTPS.
EXCHANGE_USER_DOMAIN	String	Null	Specifies the user domain for Microsoft Exchange Server.
EXCHANGE_SERVER_LIST	String	Null	Specifies the list containing IP or DNS address of Microsoft Exchange Server. Use the parameter if the automatic synchronization fails.

IP Office parameters

Parameter	Type	Default value	Description
ENABLE_IPOFFICE	Integer	0	Specifies the environment for deployment. Assign one of the following values: • 0: Non IP Office environment. • 1: IP Office environment.
SUBSCRIBE_LIST_NON_AVAYA	String	reg, message-summary, avaya-ccs-profile	Specifies the event package list for subscription after registration.

Chapter 5: Configuration through the Settings app

Navigating to the Settings screen

Procedure

Activating the Settings app in the administrator mode

About this task

You can activate the Settings app in the administrator mode. In the administrator mode, the Settings app displays all menu items that are not otherwise displayed to a user, for example, network configuration menu. If you start the Settings app when the Collaboration Station is locked, you can start the app only in the administrator mode.

Procedure

1. Go to the Settings screen.

2. Tap **Menu** > **Admin login** in the upper-right corner of the screen.
3. Enter the administrator password.

Network configuration

Configuring the Ethernet settings

Procedure

1. Open the Settings app in the admin mode.
2. Tap **WIRELESS & NETWORKS** > **Network** > **Ethernet**.
3. Tap **Menu** > **Admin login**.
4. Enter the administrator password.
5. Update the Ethernet fields.
6. To save the updates, quit the Settings app.

Ethernet settings field descriptions

Name	Description
Interfaces	
Ethernet	Specifies the Ethernet mode.
PC Ethernet	Specifies the PC Ethernet mode.
IEEE 802.1x authentication	
Supplicant mode	
Pass through mode	Specifies the pass through mode.
EAP Type	Specifies the EAP type.
802.1x credentials	Specifies the 802.1x credentials-identity and password.
LLDP	
LLDP Mode	Specifies the mode for LLDP. Choose one of the following options: • Disabled • Enabled • Auto
Received LLDP port description	Specifies the status that whether the LLDP port description is received.

Table continues…

Name	Description
Received LLDP system name	Specifies the status that whether the LLDP system name is received.
Received LLDP system description	Specifies the status that whether the LLDP system description is received.
Received LLDP management address	Specifies the status that whether the LLDP management address is received.
VLAN	
VLAN tagging (802.1Q)	Specifies the VLAN tagging mode.
VLAN	Specifies the VLAN ID.
VLAN test timer	Specifies the VLAN test timer.
IP interface	
Use DHCP	Specifies whether to use DHCP to automatically generate the IP address.
Static IP settings	Specifies the fields for assigning static IP address.
Power over Ethernet (PoE)	
Single port PoE injector connected	Specifies whether Single port PoE injector is connected to the device.
Max PoE power (watts)	Specifies the maximum power for the PoE.

Static IP settings

Name	Description
IP Address	Specifies the IP address.
Netmask	Specifies the netmask.
Default router	Specifies the default router.

Debugging and monitoring the device

Configuring the SSH server settings

Procedure

1. Open the settings app in the admin mode.
2. Tap **SYSTEM** > **Debugging and monitoring options** > **SSH server settings**.
3. Select the **SSH server mode** check box to enable Secure Shell with challenge or response authentication.

Configuring the log settings

Procedure

1. Open the settings app in the admin mode.
2. Tap **SYSTEM** > **Debugging and monitoring options** > **Log**.
3. Tap **Log Categories** to select log categories.
4. Tap **Remote Logging** to configure parameters for system logging.
5. Tap **Local Logging** to configure parameters for local logging.

Configuring port mirroring

About this task

Use the following procedure to copy the Ethernet packets that are transmitted or received on the network to the personal computer port.

Procedure

1. Open the settings app in the admin mode.
2. Tap **SYSTEM** > **Debugging and monitoring options**.
3. Select the **Port mirroring** check box to enable port mirroring.

Enabling debugging through console port

Procedure

1. Open the settings app in the admin mode.
2. Tap **SYSTEM** > **Debugging and monitoring options**.
3. Select the **Console port** check box to enable the debugging through console port.

Generating a debug report

About this task

Use the following procedure to generate a debug report. You can save the report in the internal flash memory of the Collaboration Station or an HTTP or HTTPS server. Ensure that the debug password is recorded properly as the report is encrypted and cannot be decrypted without the password.

Procedure

1. Go to the Settings screen.

2. Tap **SYSTEM** > **Debugging and monitoring options** > **Debug report** > **Generate debug report**.
3. Enter the password and select the destination location.
4. Tap **Generate**.

Pinging a device on the network

Procedure

1. Go to the Settings screen.
2. Tap **SYSTEM** > **Debugging and monitoring options** > **Host to ping**.
3. Enter the IP address or host name of the device.
4. Tap **OK**.

   The Collaboration Station displays the ping messages if the station resolves the IP address.

Tracing the route of a device

Procedure

1. Go to the Settings screen.
2. Tap **SYSTEM** > **Debugging and monitoring options** > **Trace route**.
3. Enter the IP address or the host name of the device.
4. Tap **OK**.

   The Collaboration Station displays the hops in case the station resolves the IP address.

Chapter 6: Configuration through LLDP

LLDP overview

Link Layer Discovery Protocol (LLDP) is an open standards layer 2 protocol that IP deskphones 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.

The transmission and reception of LLDP is specified in IEEE 802.1AB-2005. The Avaya H100-Series Video Collaboration Stations 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).

The Avaya H100-Series Video Collaboration Stations running SIP software support IEEE 802.1AB if the value of the configuration parameter LLDP_ENABLED is "1" (On) or "2" (Auto). If the value of LLDP_ENABLED is "0" (off), the transmission and reception of Link Layer Discovery Protocol (LLDP) is not supported. When the value of LLDP_ENABLED is "2", the transmission of LLDP frames will not begin until or unless an LLDP frame is received, and the first LLDP frame will be transmitted within 2 seconds after the first LLDP frame is received. Once transmission begins, an LLDPDU will be transmitted every 30 seconds. There could be a delay of up to 30 seconds in deskphone initialization if the file server address is delivered by LLDP and not by DHCP.

These deskphones:

- Do not support LLDP on the secondary Ethernet interface.
- Will 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 Avaya H100-Series Video Collaboration Stations initiates LLDP after receiving an LLDPDU message from an appropriate system. Once initiated, the devices send an LLDPDU every 30 seconds with the contents described in LLDPDU transmitted by the SIP devices.

LLDPDU transmitted by the deskphones

Category	TLV Name (Type)	TLV Info String (Value)
Basic Mandatory	Chassis ID	IPADD of deskphone, IANA Address Family Numbers enumeration value for IPv4, or subtype 5:Network address.
Basic Mandatory	Port ID	MAC address of the device.
Basic Mandatory	Time-To-Live	120 seconds.
Basic Optional	System Name	The Host Name sent to the DHCP server in DHCP option 12.
Basic Optional	System Capabilities	Bit 2 (Bridge) will be set in the System Capabilities if the deskphone has an internal Ethernet switch. If Bit 2 is set in Enabled Capabilities then the secondary port is enabled.
Basic Optional	Management Address	Mgmt IPv4 IP address of device. Interface number subtype = 3 (system port). Interface number = 1. OID = SNMP MIB-II sysObjectID of the device.
IEEE 802.3 Organization Specific	MAC / PHY Configuration / Status	Reports autonegotiation status and speed of the uplink port on the device.
TIA LLDP MED	LLDP-MED Capabilities	Media Endpoint Discovery capabilities = 00-33 (Inventory, Power-via-MDI, Network Policy, MED Caps).
TIA LLDP MED	Network Policy	Tagging Yes/No, VLAN ID for voice, L2 Priority, DSCP Value.
TIA LLDP MED	Inventory – Hardware Revision	MODEL - Full Model Name.
TIA LLDP MED	Inventory – Firmware Revision	Firmware version .
TIA LLDP MED	Inventory – Software Revision	APPNAME.
TIA LLDP MED	Inventory – Serial Number	Device serial number.
TIA LLDP MED	Inventory – Manufacturer Name	Avaya.
TIA LLDP MED	Inventory – Model Name	MODEL with the final Dxxx characters removed.
Avaya Proprietary	Call Server IP address	Call Server IP Address. Subtype = 3
Avaya Proprietary	IP Phone addresses	Phone IP address, Phone Address Mask, Gateway IP Address. Subtype = 4.
Avaya Proprietary	File Server	File Server IP Address. Subtype = 6.
Avaya Proprietary	802.1Q Framing	802.1Q Framing = 1 if tagging or 2 if not.
Basic Mandatory	End-of-LLDPDU	Not applicable.

TLV impact on system parameter values

System parameter name	TLV name	Impact
PHY2VLAN	IEEE 802.1 Port VLAN ID	The value 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 is set to 1 (ON). A check is made as to whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. VLAN Name TLV is ignored if: • The value of USE_DHCPis "0" and the value of IPADD is not "0.0.0.0". • The current value of L2QVLAN was set by a TIA LLDP MED Network Policy TLV. • The VLAN name in the TLV does not contain the substring "voice" in lower-case, upper-case or mixed-case ASCII characters anywhere in the VLAN name.
L2Q, L2QVLAN, L2QAUD, DSCPAUD,	TIA LLDP MED Network Policy (Voice) TLV	L2Q - set to "2" (off) if T (the Tagged Flag) is set to 0 and to "1" (on) if T is set to 1. L2QVLAN - Set to the VLAN ID in the TLV. L2QAUD - Set to the Layer 2 Priority value in the TLV. DSCPAUD - Set to the DSCP value in the TLV. A check is made as to whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. This TLV is ignored if: • The value of USE_DHCP is "0" and the value of IPADD is not "0.0.0.0". • The Application Type is not 1 (Voice) or 2 (Voice Signaling). • The Unknown Policy Flag (U) is set to 1.
VLAN_IN_USE, L2QSIG, DSCPSIG	TIA LLDP MED Network Policy (Voice Signaling)	VLAN_IN_USE - set to the VLAN ID in the TLV. If the Layer 2 Priority value in the TLV is not zero, and if the Application Type is 2 (Voice Signaling), L2QSIG is set to the Layer 2 Priority value in the TLV. If the DSCP value in the TLV is not zero, and if the Application Type is 2 (Voice Signaling), DSCPSIG is set to the DSCP value in the TLV.

Table continues…

System parameter name	TLV name	Impact
		This TLV is ignored if: • The value of USE_DHCP is "0" and the value of IPADD is not "0.0.0.0". • The Application Type is not 1 (Voice) or 2 (Voice Signaling). • The Unknown Policy Flag (U) is set to 1.
SIP_CONTROLLER_LIST	Proprietary Call Server TLV	SIP_CONTROLLER_LIST will be set to the IP addresses in this TLV value. **Note:** This parameter cannot be used in an environment where both SIP deskphones and H.323 deskphones exist.
TLSSRVR and HTTPSRVR	Proprietary File Server TLV	FILE_SERVER_URL will be set to the IP addresses in this TLV value.
L2Q	Proprietary 802.1 Q Framing	If TLV = 1, L2Q set to "1" (On). If TLV = 2, L2Q set to "2" (Off). If TLV = 3, L2Q set to "0" (Auto). A check is made as to whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. This TLV is ignored if: • The value of USE_DHCP is "0" and the value of IPADD is not "0.0.0.0". • The current L2QVLAN value was set by an IEEE 802.1 VLAN name. • The current L2QVLAN value was set by a TIA LLDP MED Network Policy (Voice) TLV.

Chapter 7: Load and patch management

Device upgrade

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

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

For more information on the software download and the device upgrade, see *Installing and Maintaining Avaya H100-Series Video Collaboration Stations*.

Chapter 8: Security

Avaya H100-Series Video Collaboration Stations provide lock and logout functions for security and protection of the privacy of a user. When a user locks the Collaboration Station, no one can unlock the station without the assigned password for the particular user. When the Collaboration Station is in a locked state, a user can receive calls or make emergency calls. The Collaboration Station restricts access to any user data while in locked state.

When a user logs out from the Collaboration Station, the station is available for other users to use. However, when another user logs in to the same station, that user cannot access other user's data as the Collaboration Station deletes all data of the previous user. For example, suppose user A and user B use the same Collaboration Station and user B logs into the same station when the user A logs out. The user B cannot access any record of the user A, such as contacts and call records, on the Collaboration Station.

For troubleshooting, the Collaboration Station support SSH and a secure challenge/response mechanism for the Avaya professionals to login to the station remotely and perform the required operations remotely in a secure environment. SSH users are not given the root access. The SSH user access privileges do not support access to any user private data or information including:

- Digital certificate private keys.
- Authentication credentials for SIP, HTTP, 802.1X, and Exchange.
- Contact and call log information.
- Personal browser information, such as bookmarks, URL history, and cookies.

To enhance security, the Collaboration Station supports Secure Real-time Transport Protocol (SRTP), which is based on AES-128 and AES-256. SRTP provides confidentiality and message authentication to media traffic going over the LAN infrastructure. This allows the Collaboration Station to encrypt the calls between two or more endpoints, to restrict anyone from eavesdropping.

In order to correctly use SRTP, there are various components within the network that you must correctly configure. For the Collaboration Station to function properly with SRTP, you must configure the equivalent parameters in Communication Manager or System Manager. You must configure the following three parameters on the Collaboration Station and the equivalent Communication Manager parameters must match:

- SET ENFORCE_SIPS_URI 1
- SET SDPCAPNEG 1
- SET MEDIAENCRYPTION X,9
- SET MEDIAENCRYPTION X , where X is a value from 1 to 11

The Collaboration Station notifies you whenever you are in a secure call, using TLS and SRTP. The Collaboration Station provides call status information in the call statistics. The call status provides information about secure call and that the call is encrypted. The support for Transport Layer Security (TLS) allows the Collaboration Station to establish a secure connection to a HTTPS server, in which the upgrade and settings file can reside. Communications between the Collaboration Station and the Personal Profile Manager (PPM) can also be secured by setting the CONFIG_SERVER_SECURE_MODE parameter.

Index

S

T

U

V