# Installing and Maintaining 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 preparing the Avaya H100-Series Video Collaboration Stations for installation, deployment, initial administration, maintenance and troubleshooting.

## Intended audience

This document is intended for people who install and maintain the Avaya H100-Series Video Collaboration Stations. Before deploying the product, ensure that you have the following knowledge, skills, and tools:

**Knowledge**

- DHCP
- SIP
- Installing and configuring Avaya Aura® components
- Installing and configuring IP Office components

**Skills**

How to administer and configure:

- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Presence Services
- Avaya Aura® Session Border Controller
- Avaya Aura® Conferencing
- Avaya Scopia®
- IP Office
- DHCP server
- HTTP or HTTPS server
- Microsoft Exchange Server

**Tools**

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

# Related resources

## Documentation

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

| 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. |
| *Avaya Aura® Session Manager Overview and Specification* | See characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security and licensing requirements of the Avaya Aura® Session Manager. | For people who want to gain a high-level understanding of the Avaya Aura® Session Manager features, functions, capacities, and limitations. |
| Implementing | | |
| *Deploying Avaya Aura® Session Manager* | See the installation procedures and initial administration information for Avaya Aura® Session Manager. | For people who install, configure, and verify Avaya Aura® Session Manager on Avaya Aura® System Platform. |
| *Upgrading Avaya Aura® Session Manager* | See upgrading checklists and procedures. | For people who perform upgrades of Avaya Aura® Session Manager. |

*Table continues…*

| Title | Use this document to: | Audience |
|---|---|---|
| *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. |
| *Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager* | See the installation procedures and initial administration for IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager. | For people who install and configure IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager. |
| *Installing and Maintaining Avaya IP Office™ Platform Application Server* | See the installation procedures and initial administration for IP Office™ Platform Application Server. | For people who install and configure IP Office™ Platform Application Server. |
| 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 H100-Series Video Collaboration Stations* | See 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. | For people who perform Avaya H100-Series Video Collaboration Stations system administration tasks such as backing up and restoring data and managing users. |
| *Administering Avaya Aura® Session Manager* | See information about how to perform Avaya Aura® Session Manager administration tasks including how to use management tools, how to manage data and security, 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® |

*Table continues…*

| Title | Use this document to: | Audience |
|---|---|---|
| | | Conferencing administration tasks. |
| Avaya Scopia® Management Administrator Guide | See information about how to perform Avaya Scopia® administration tasks. | For people who perform Avaya Scopia® administration tasks. |
| *Administering Avaya IP Office™ Platform with Manager* | See information about how to perform Avaya IP Office™ Platform with Manager tasks. | For people who perform Avaya IP Office™ Platform with Manager tasks. |
| *Administering Avaya IP Office™ Platform with Web Manager* | See information about how to perform Avaya IP Office™ Platform with Web Manager tasks. | For people who perform Avaya IP Office™ Platform with Web Manager 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. |

**Related links**

Finding documents on the Avaya Support website on page 11

## Finding documents on the Avaya Support website

### About this task

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

### Procedure

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

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

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

**Related links**

Documentation on page 9

# 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 14
Product compatibility on page 17
Packaged components on page 17
Connectors and controls on page 18

# 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.<br>• 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.<br>• H.264 AVC baseline and high profile.<br>• Support external monitors with resolutions up to 1080p.<br>• Zero latency, display pass-through with Picture-in-Picture functionality for sharing an external monitor with a computer.<br>• User control for video window size and position.<br>• 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.<br>• Bright, f2.0 lens for a superior performance in low light.<br>• Camera that can be mounted on the device or on an external monitor.<br>• Mechanical privacy shutter. |

*Table continues…*

| | | |
|---|---|---|
| | | • Activity LED. |
| | Handset | • Wireless handset, which is available in specific countries, supports DECT 6.0 and has call control, mute, and volume buttons.<br>• Optional wired handset. |
| | Physical security | Kensington security slot. |
| | Physical buttons and LEDs | • Dialpad: 0-9, *, and #.<br>• Volume up and volume down buttons.<br>• Audio mute and video block buttons.<br>• Speakerphone and headset buttons.<br>• Message Waiting Indicator LED.<br>• LED touch buttons. |
| | Connectors | • RJ45 primary Gigabit Ethernet (10/100/1000 Mbps) PoE LAN port.<br>• RJ45 secondary Gigabit Ethernet (10/100/1000 Mbps) port for personal computer.<br>• USB dedicated camera port.<br>• USB 2.0 charging port with up to 1.5 A power to rapidly recharge smartphones and tablets.<br>• Two USB 2.0 general purpose ports.<br>• USB 2.0 micro AB port.<br>• Digital display video output port capable of supporting a monitor with up to 1080p.<br>• Digital display input port capable of handling digital video from a personal computer for picture-in-picture video overlay support.<br>• RJ9 analog handset port.<br>• RJ9 analog headset port.<br>• SD card slot is not currently supported.<br>• 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. |
| | Bluetooth | Supports:<br>• Bluetooth 4.0.<br>• Headset profile. |

*Table continues…*

| | | |
|---|---|---|
| **Power** | Ethernet | • IEEE 802.3at.<br>• Single Port PoE injector (SPPoE). |
| | AC power | External 30 W AC power adapter. |
| **Accessory support** | - | • USB headset, keyboard, and mouse.<br>• Bluetooth HID-keyboard and mouse.<br>• Bluetooth headsets. |
| **Software features** | - | • Android 4.3 operating system.<br>• Avaya Aura® features.<br>- Audio and video call management.<br>- Advanced call management, such as call forwarding, call transfer, call park, and bridged call appearances.<br>• IP Office v10.0 features.<br>- Audio and video call management.<br>- Synchronize user contacts with Avaya one-X® Portal.<br>• Audio and video call with Avaya Scopia® Elite MCU and Avaya Aura® Conferencing with roster control.<br>• Microsoft Exchange Server calendar and contacts integration.<br>- Microsoft Exchange Server calendar integration with built-in click-to-call support.<br>• Contact app<br>- Synchronize contacts with Microsoft Exchange Server .<br>- Synchronize user contacts with Avaya Aura® System Manager.<br>- Synchronize user contacts with Avaya one-X® Portal.<br>• Publish and display presence status with Avaya Aura® Presence Services integration.<br>• Enhanced user interface shared with Avaya Communicator 2.0 optimized for touchscreen.<br>• HTML 5 browser with built-in click-to-call support.<br>• History, Calculator, and Alarm clock apps.<br>• Online help. |
| **Security** | | • Screen lock facility.<br>• 802.1x EAP-TLS and EAP-MD5 over the Ethernet interface.<br>• Wi-Fi WEP, WPA/WPA2 PSK, and 802.1x EAP, where for 802.1x EAP following features are supported:<br>- EAP-PEAP with MSCHAPV2 and EAP-GTC as phase 2 authentication methods. |

*Table continues…*

| | | |
|---|---|---|
| | | - EAP-TLS.<br>- EAP-TTLS with MSCHAP, MSCHAPV2, and EAP-GTC as phase 2 authentication methods.<br>- EAP-PWD.<br>• Trusted certificate repository configured through the settings file to be used by all applications.<br>• Android built in certificates are used in addition to trusted certificates for the browser and Microsoft Exchange Server.<br>• Identity certificate generation using SCEP.<br>• Support SIP signaling over TLS.<br>• Media encryption (SRTP) using AES-128 and AES-256.<br>• Supports SRTCP (authentication only).<br>• 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 13

# 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 13

# Packaged components

Ensure that the package contains the following parts:

- The Collaboration Station base
- Wireless handset
- Two AAA rechargeable batteries
- Ethernet cable
- Camera
- 2-meter USB cable

The camera and USB cable are packaged in a separate box.

The package might also contain the following optional components:

- Wired handset with a handset cord
- Charging pins cover

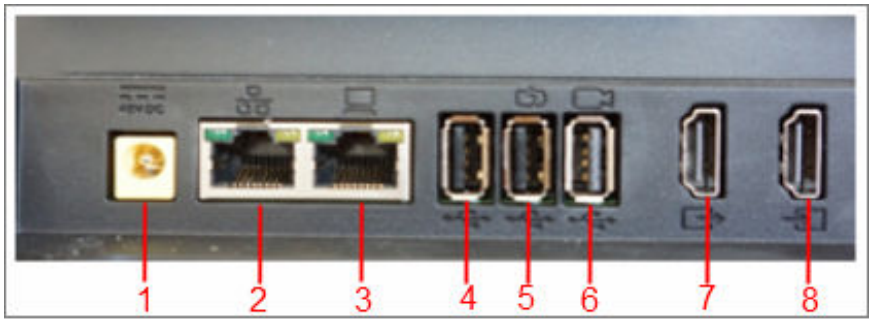
You might also get a package of an AC power adapter and cord if you ordered one for the device.

**Related links**

Avaya H100-Series Video Collaboration Stations overview on page 13

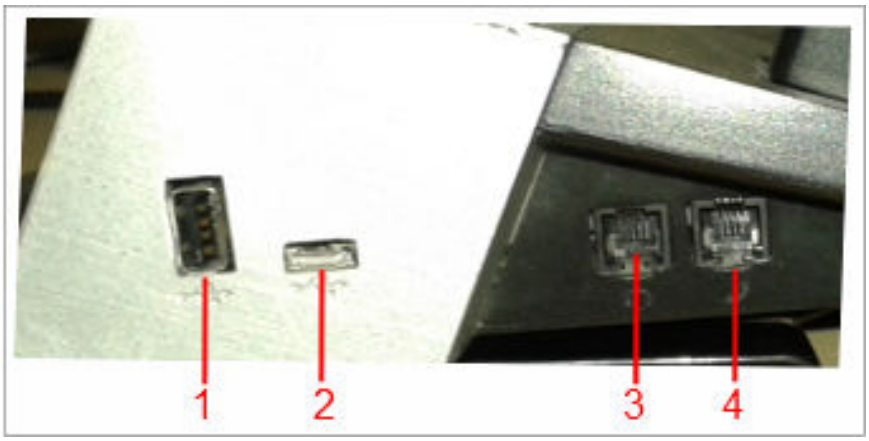
# Connectors and controls

## Rear Panel




| Number | Name |
|---|---|
| 1 | Power connector |
| 2 | RJ45 10/100/1000 Mbps Gigabit Ethernet connector |
| 3 | RJ45 10/100/1000 Mbps Gigabit Ethernet personal computer connector |
| 4 | USB 2.0 connector |
| 5 | USB 2.0 high-power gadget charging connector<br>As the port uses only the spare power, the charging speed may vary based on whether power supply is through AC, PoE, or SP-PoE |
| 6 | USB camera connector |
| 7 | Digital video display out connector |
| 8 | Digital video display in connector |

### Side panel




| Number | Name |
|---|---|
| 1 | USB 2.0 connector |
| 2 | USB 2.0 micro AB connector |
| 3 | RJ9 analog headset connector |
| 4 | RJ9 analog handset connector |

### Front panel


| Number | Name |
|---|---|
| 1 | SD card slot that is currently not supported |

### Related links

Avaya H100-Series Video Collaboration Stations overview on page 13

# Chapter 3: Initial setup and connectivity

## Installation checklist

Use the following checklist to see the tasks that you must perform to install Collaboration Station.

| No. | Task | Reference | ✔ |
|---|---|---|---|
| 1. | Check the prerequisites. | See Prerequisites on page 20. | |
| 2. | Gather preinstallation data. | See Preinstallation data gathering on page 21. | |
| 3. | Configure the servers. | See Server configurations on page 24. | |
| 4. | Configure the settings file. | See Configuring the settings file on page 39. | |
| 5. | Create users on Avaya Aura® System Manager. | See Creating users on System Manager on page 27. | |
| 6. | Create users on IP Office Web Manager . | See *Administering Avaya IP Office™ Platform with Web Manager*. | |
| 7. | Assemble the Collaboration Station. | See Assembling the Collaboration Station on page 27. | |
| 8. | Connect the Collaboration Station to the network. | See Connecting the Collaboration Station to the network on page 33. | |

## Prerequisites

Check the prerequisites to ensure that you have the required software and hardware before you install the Collaboration Station.

### Software requirements

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

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

- Avaya Aura® Presence Services 6.2.4 or later
- Avaya Aura® Session Border Controller 7.0 and 7.0.1
- IP Office 10.0 or later
- A DHCP server for providing dynamic IP addresses to the Collaboration Station.
- A file server, an HTTP, HTTPS, or the Avaya Utility server for downloading the software distribution package and the settings file
- One or both of the following conference servers for both audio and video conference:
  - Avaya Aura® Conferencing 8.0 or later
  - Avaya Scopia® Elite MCU

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

**Related links**

Documentation on page 9

## Hardware requirements

Ensure that the LAN:

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

If your network does not have a 802.3at PoE or 802.3af PoE injector specification, you can power the deskphone using the AC power adapter that you can order with the device.

# Preinstallation data gathering

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

## System Manager user profile worksheet

For creating user profile on System Manager.

### Identity tab

| Field | Value | Notes |
|---|---|---|
| Last Name | | |
| Login Name | | |
| Password | | |
| Localized Display Name | | |
| Endpoint Display Name | | |
| Language Preference | | |
| Time Zone | | |

### Communication Profile tab

| | Field | Value | Notes |
|---|---|---|---|
| Communication Profile section | | | |
| | Communication Profile Password | | |
| Communication Address section | | | |
| | Handle Types are for:<br>• Avaya SIP<br>• Avaya E.164<br>• Avaya Presence/IM if Presence is used | | |
| | Handle Fully Qualified Address | | |
| Session Manager Profile section | | | |
| | Primary Session manager | | |
| | Secondary Session Manager | | |
| | Origination Application Sequence | | |
| | Termination Application Sequence | | |
| | Survivability Server | | |
| | Home Location | | |
| CM Endpoint Profile section | | | |

*Table continues…*

| | Field | Value | Notes |
|---|---|---|---|
| | System | | |
| | Profile Type | | |
| | Use Existing Endpoints | | |
| | Extension | | |
| | Endpoint Template | | |
| | Voice Mail Number | | |
| Messaging Profile section | | | Optional |
| | System | | |
| | Mailbox Number | | |
| | Template | | |
| | Password | | |
| | Delete Subscriber on Unassign and Delete | | |

## Settings file worksheet

For initial deskphone configuration, gather values for the following parameters.

| Field | Value | Notes |
|---|---|---|
| ISO_SYSTEM_LANGUAGE | | |
| TIMEFORMAT | | |
| TIMEZONE | | |
| COUNTRY | | |
| SIP_CONTROLLER_LIST | | |
| SIPDOMAIN | | |

**Note:**

In an IP Office environment, `H1xxsettings.txt` settings and `H1xxSupgrade.txt` upgrade files are auto-generated. There is also a provision where you can setup a different file server with your own custom settings file.

## DHCP settings worksheet

For dynamically assigning IP addresses to the deskphones and any initial configuration that is required through DHCP options.

| Field/Parameter | Value | Notes |
|---|---|---|
| Range of IP addresses | | |
| DHCP options | | |
| HTTPSRVR | | |
| TLSSRVR | | |
| FILE_SERVER_URL | | |

# Server configuration

To install the Collaboration Station, you need to configure the following servers:

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

**Note:**

In an IP Office environment, `H1xxsettings.txt` settings and `H1xxSupgrade.txt` upgrade files are auto-generated. There is also a provision where you can setup a different file server with your own custom settings file.

**Related links**

DHCP server configuration on page 24
File server configuration on page 25

# DHCP server configuration

Configure the DHCP server to:

- Dynamically assign IP addresses to the Collaboration Station.
- Provision device and site-specific configuration parameters through various DHCP options.

For more information about the device and site-specific configuration parameters, see *Administering Avaya H100-Series Video Collaboration Stations*.

**Related links**

Server configuration on page 24
Setting up a DHCP server on page 24

## Setting up a DHCP server

### Procedure

1. Install the DHCP server software according to the vendor instructions.

2. Configure the range of IP address available to the Collaboration Station.
3. Configure the required DHCP options.

**Related links**

DHCP server configuration on page 24

# File server configuration

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

Deskphones can download the software distribution package, firmware image, and configuration file using the HTTP server and the settings file using an HTTP or HTTPS server.

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

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

- DHCP
- LLDP
- Device interface
- Settings file

For LLDP, DHCP, and the settings file, you can assign the file server address to the FILE_SERVER_URL parameter. You can also specify the file server address in the HTTPSRVR and TLSSRVR parameters. If the value of the file server address is set in more than one parameter, the deskphone uses the value specified in the FILE_SERVER_URL parameter and ignores other parameter.

**Related links**

Server configuration on page 24
Software distribution package on page 25
Setting up a file server on page 26
Downloading and saving the software on page 26

## Software distribution package

The software distribution package includes:

- Signed Software Package files
- An upgrade file named `H1xxSUpgrade.txt`
- A file named `av_prca_pem_2033.txt` that contains a copy of the Avaya Product Root Certificate Authority certificate in PEM format
- A file named `av_sipca_pem_2027.txt` that contains a copy of the Avaya SIP Root Certificate Authority certificate in PEM format

- A directory named `signatures` that contains signature files and a Signing Authority Certificate file named `RootSA.txt`

**Related links**

File server configuration on page 25

## Setting up a file server

### Procedure

1. Install the HTTP or HTTPS server software according to the vendor instructions.
2. Download and save the software distribution package and the settings file at the appropriate location on the server.
3. Unzip the distribution package and save the extracted files at an appropriate location on the server.
4. Open and modify the settings file to provision the required device configuration parameters.

**Related links**

File server configuration on page 25

## Downloading and saving the software

### Before you begin

Ensure that your file server is set up.

### Procedure

1. Go to the Avaya Support website.
2. In the **Enter Your Product Here** field, enter `Avaya H100-Series Video Collaboration Stations`.
3. In the **Choose Release** field, click the required release number.
4. Click the **Downloads** tab.

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

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

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

**Related links**

File server configuration on page 25

# Creating users on Avaya Aura® System Manager

### Procedure

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

   The phone type must be 9641SIP.
8. Perform the following steps to enable the video calls.
   a. In the **CM Endpoint Profile** section, click **Endpoint Editor** > **Feature Options**.
   b. In the **Features** area, select the **IP Video** check box.
   c. Click **Done**.
9. Click **Commit & Continue**.

# Assembling the Collaboration Station

**Related links**

Connecting a wired handset on page 27
Wireless handset on page 28

## Connecting a wired handset

### About this task

If you bought the Collaboration Station with a wireless handset and now want to replace the wireless handset with a wired handset, then you must cover the pins as described in this task. If you ordered the Collaboration Station with a wired handset, the charging pins are covered and you only need to connect the handset.

You cannot use the wireless handset if you connect a wired handset.

### Procedure

1. Perform the following steps only if you are replacing the wireless handset with the wired handset, else skip the steps.
   a. From the back of the device, remove the screw that is below the charging pins bushing.
   b. Remove the charging bushing plastic.
   c. Attach the blind bushing plastic cover from the top and secure it with a screw.
2. Plug non-spiral end of the handset cord into the handset connector on the Collaboration Station.
3. Plug the other end into the connector in the handset.
4. Disable the wireless handset.

**Related links**

Assembling the Collaboration Station on page 27

---

# Wireless handset

Install the wireless handset only if it is supported in the country where you are installing the device. The wireless handset is supported in the following countries:

- Australia
- Austria
- Argentina
- Belgium
- Bulgaria
- Brazil
- Canada
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Finland
- France
- Germany
- Greece
- Hong Kong
- Hungary

- Iceland
- Ireland
- Israel
- Italy
- Liechtenstein
- Luxembourg
- Japan
- Korea
- Mexico
- Netherlands
- Norway
- Poland
- Portugal
- Romania
- Russia
- Saudi Arabia
- Slovakia
- Slovenia
- Sweden
- Switzerland
- Spain
- Taiwan
- United Kingdom
- USA

**Related links**

Assembling the Collaboration Station on page 27
Wireless handset layout on page 30
Installing the wireless handset on page 31

## Wireless handset layout


| Number | Name |
|---|---|
| 1 | **Mute** |
| 2 | **Volume up** |
| 3 | **Volume down** |
| 4 | **Battery slot** |
| 5 | **Charging pins** |
| 6 | **Mute LED** |
| 7 | **Call control** |

### Related links

Wireless handset on page 28

## Installing the wireless handset

### Before you begin

Ensure that the administrator configured the country settings and enabled the DECT menu option for the wireless handset. Once you have installed the wireless handset, the batteries will take around 16 hours to get fully charged for the first time.

### Procedure

1. Set the COUNTRY parameter in the settings file to an appropriate value.

   In an IP Office environment, if you are using the auto-generated settings file, the wireless handset is registered according to the country specified in the IP Office server.

2. Ensure that the DECTSTAT parameter is set to 1 to enable the DECT menu option in the Settings file.
3. Install the batteries in the battery slot by matching the poles as shown in the slot label.

   **Danger:**

   There is a risk of explosion if you use an incorrect type of battery.

4. Put the wireless handset in the cradle.

   The Collaboration Station displays the battery level and the pairing information in the Top Bar.

**Related links**

Wireless handset on page 28

# Camera

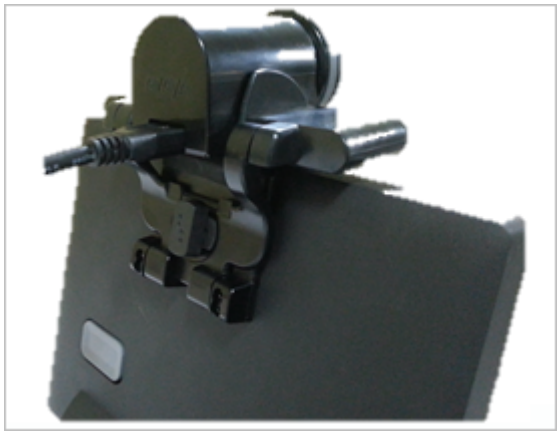
## Camera mount

The camera supports the following mount options:

- Integrated mount
- External mount

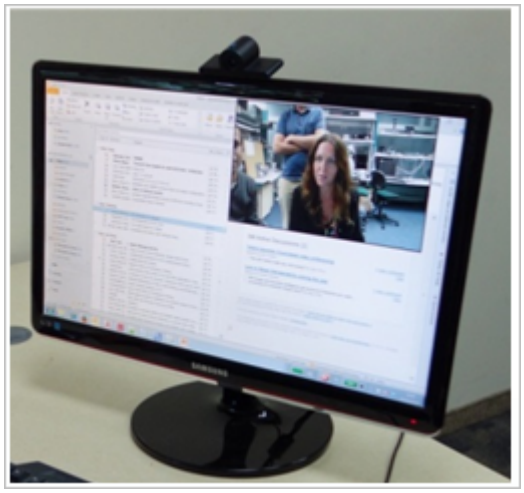
### Integrated mount

The camera is mounted on the Collaboration Station itself. The following image shows the camera mounted on the Collaboration Station.



### External mount

The camera can be mounted on an external monitor so that the user can view the video calls on the connected monitor. The following image shows the camera mounted on an external monitor.



**Related links**

Assembling the Collaboration Station on page 27

## Mounting and connecting the camera

### Procedure

- For integrated mount:
  1. Position the camera on the Collaboration Station.
  2. Fold the camera leg and insert the camera latch in the twist lock at the back of the Collaboration Station.
  3. Plug one end of the camera cable into the camera connector of the Collaboration Station. Plug the other end into the connector in the camera.

- For external mount:
  1. Position the camera on the external monitor and open the camera leg to balance the camera properly.
  2. Plug one end of the camera cable into the camera connector of the Collaboration Station. Plug the other end into the connector in the camera.
  3. Plug one end of the video cable into the video display out connector of the Collaboration Station. Plug the other end into the video display in connector of the external monitor.

**Related links**

Assembling the Collaboration Station on page 27

# Connecting the Collaboration Station to the network

## About this task

You can connect your Collaboration Station to an Ethernet or a Wi-Fi network. The Wi-Fi option is enabled by default in the settings file.

If you connect to a Wi-Fi network that has a Captive portal enabled, the Collaboration Station displays a notification in the Top Bar to sign into to the Wi-Fi network. Tapping the notification in the Top Bar opens the Captive portal page where you need to provide the login details to login to the network.

## Procedure

1. If your are connecting the deskphone to a wireless network or a wired network that does not have a 802.3at PoE or 802.3af PoE injector specification, connect the power adapter to the 48–V DC power connector at the back of the Collaboration Station and plug the power adapter into an electrical outlet.
2. Perform one of the following actions:
   - To connect to a wired network, plug one end of an Ethernet cable into the LAN connector at the back of the Collaboration Station. Plug the other end into an available LAN port.
   - To connect to a wireless network:
     a. Wait for the deskphone to initialize and display the LOGIN screen.
     b. Tap the Settings icon.
     c. Tap **WIRELESS & NETWORKS** > **Network** > **Network mode** > **Wi-Fi**.
     d. Tap **Wi-Fi** and select a network from the list of networks.
     e. Enter the login credentials that the Collaboration Station displays if the Wi-Fi network is a secured network.

# Chapter 4: Security configurations

## Device lock configuration

The Avaya H100-Series Video Collaboration Stations provide the device lock features for securing user privacy. When a user locks the Collaboration Station, other users cannot unlock the device without the assigned password of the device. A user can receive calls or make emergency calls even if the Collaboration Station is in the locked state.

The lock screen password is the same as the login password that is used for registering the Collaboration Station. Ensure that you create different passwords for each user profile.

To enable the device lock feature, configure the following parameter in the settings file.

| Parameter | Set to | Notes |
|---|---|---|
| ENABLE_PHONE_LOCK | 1 | User can manually lock the device or the device locks itself if there is screen inactivity for the amount of time specified in the PHONE_LOCK_IDLETIME parameter.<br>Collaboration Station can be configured to lock enable and the user cannot disable the exchange policy if the Exchange account is configured.<br>**Note:**<br>In an IP Office environment, the default value is set to 0 in the auto-generated settings file. |

## Password security policies

If you plan to configure the Exchange account on the Collaboration Stations, you can also provide secure device access by configuring the password security policies on Microsoft Exchange Server. If you configure the password policies, ensure that the device password complies with these policies. If the device password does not comply with the policies, the Exchange account configuration on the device fails.

# Certificate management

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

- SIP/TLS: Uses the trusted certificates if the certificates are configured, else uses the default Avaya SIP Product CA certificate. The identity certificate generated using SCEP is used if the deskphone identity certificate is requested by Avaya Aura® Session Manager for mutual authentication or when the CONNECTION_REUSE parameter is set to 0 and the deskphone listens to inbound connections from Avaya Aura® Session Manager.
- PPM/HTTPS/TLS: Uses the trusted certificates if the certificates are configured, else uses the default Avaya SIP Product CA certificate. The identity certificate generated using SCEP is used if the deskphone identity certificate is requested by PPM for mutual authentication.
- Software distribution package and settings file downloaded from the HTTPS server: Uses the trusted certificates if the certificates are configured, else uses the Avaya Product Root CA certificate. The identity certificate generated using SCEP is used if the deskphone identity certificate is requested by the file server for mutual authentication.
- Ethernet 802.1x EAP-TLS: Uses the trusted certificates. The identity certificate generated using SCEP is used as it is required for authentication.
- Wi-Fi 802.1x EAP-TLS: Uses the trusted certificates. EAP-PEAP and EAP-TTLS might also use the trusted certificates, but for EAP-TLS the identity certificate generated using SCEP shall be used as it is required for authentication.
- Exchange using HTTPS: Uses the trusted certificates and built-in Android well known root CAs.
- Browser using HTTPS: Uses the trusted certificates and the built-in Android well known root CAs.

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

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

# Secure installation configuration

For secure installation, configure the following parameters.

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

For obtaining the downloadable files, configure the following parameters.

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

## SCEP parameters

In an IP Office environment, the following parameters are not present in the auto-generated `H1xxsettings` settings file. However, you can provision them through a custom settings file.

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

| Parameter | Type | Default value | Description |
|---|---|---|---|
| MYCERTURL | String | Null | Specifies the URL to access Simple Certificate Enrollment Protocol (SCEP) server. The device attempts to contact the server only if this parameter is set to other than its default value. |
| MYCERTCN | String | $SERIALNO | Specifies the Common name (CN) for SUBJECT in SCEP certificate request. The values can either be $SERIALNO or $MACADDR.<br>If the value includes the string "$SERIALNO”, that string will be replaced by the phones serial number.<br>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. |

*Table continues…*

| Parameter | Type | Default value | Description |
|---|---|---|---|
| MYCERTKEYLEN | Numeric | 2048 | Specifies the private key length in bits to be created in the device for a certificate enrollment. The range is from 1024 to 2048. |
| MYCERTRENEW | Numeric | 90 | Specifies the percentage used to calculate the renewal time interval out of the device certificate's Validity Object. If the renewal time interval has elapsed the phone starts to periodically contact the SCEP server again to renew the certificate. The range is from 1 to 99. |
| MYCERTWAIT | Numeric | 1 | Specifies the behavior of the device when performing certificate enrolment. assign one of the following values:<br>• 0: Periodical check in the background<br>• 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.<br>If the value contains $SERIALNO, $SERIALNO is replaced by the value of SERIALNO. If the value contains $MACADDR, $MACADDR is replaced by the value of MACADDR without the colon separators. |

## VLAN

In an IP Office environment, the following parameters are not present in the auto-generated `H1xxsettings` settings file. However, you can provision them through a custom settings file.

Configure the following VLAN parameters.

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

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

# Chapter 5: Initial administration

## Configuring the settings file

### About this task

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

### Procedure

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

**Related links**

Configuration of initial parameters on page 39
Supported countries on page 43
IP Office parameters checklist on page 49

## Configuration of initial parameters

Set the following initial parameters in the settings file. For more information and a complete list of the settings file parameters, see *Administering Avaya H100-Series Video Collaboration Stations*.

### Wireless handset

Set the following parameter for the wireless handset.

| Parameter | Type | Default value | Description |
|---|---|---|---|
| COUNTRY | String | Null | 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. |
| DECTSTAT | Integer | 1 | Specifies whether the DECT menu option in the Setting app is enabled for the user. Assign one of the following values:<br>• 0: The DECT handset and menu option is disabled in the Settings app and the user cannot change it. |

*Table continues…*

| Parameter | Type | Default value | Description |
|---|---|---|---|
| | | | • 1: The DECT handset and menu option is enabled in the Settings app and the user can change it to enable or disable the wireless handset. |

### File server

Set the following parameter to provide the file server address to the device if not configured in DHCP server.

| Parameter | Type | Default value | Description |
|---|---|---|---|
| FILE_SERVER_URL | String | Null | Specifies the configured file server URLs for downloading the software distribution package and settings files.<br>If this parameter is set, then the following parameters that are supported for the backward compatibility are ignored:<br>• HTTPSRVR<br>• HTTPPORT<br>• HTTPDIR<br>• TLSSRVR<br>• TLSSRVRDIR<br>• TLSPORT |

### Conferencing

Set the following parameter to enable Avaya Aura® Conferencing.

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

### Presence

Set the following parameter to enable the Presence services.

| Parameter | Type | Default value | Description |
|---|---|---|---|
| PRESENCE_SERVER | String | Null | Specifies the IP address of the Presence server. The range is from 0 to 255 characters. |

### SIP registration

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

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

## Time settings

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

| Parameter | Type | Default value | Description |
|---|---|---|---|
| SNTPSRVR | String | Null | Specifies a list of zero or more SNTP servers IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces. The range is from 0 to 255 characters. |
| TIMEZONE | String | Etc/GMT | Specifies the configuration of time zone in Olson format (as maintained in tzone database by IANA). |
| TIMEFORMAT | Integer | 0 | Specifies the format to display time on the device. Assign one of the following values:<br>• 0: AM/PM<br>• 1: 24 Hours |

*Table continues…*

| Parameter | Type | Default value | Description |
|---|---|---|---|
| DATE_FORMAT_OPTIONS | Integer | 1 | Specifies the format to display date on the device. Assign one of the following values:<br>• 1: Language and location specific<br>• 2: mm/dd/yyyy<br>• 3: dd/mm/yyyy<br>• 4: yyyy/mm/dd |

### Microsoft Exchange server account settings

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

| Parameter | Type | Default value | Description |
|---|---|---|---|
| EXCHANGE_USER_DOMAIN | String | Null | Specifies the user domain for Microsoft Exchange Server. |
| EXCHANGE_SERVER_SECURE_MODE | Integer | 1 | Specifies whether to use the secure mode for contacting Microsoft Exchange Server. Assign one of the following values:<br>• 0: For HTTP<br>• 1: For HTTPS |
| 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. |

**Note:**

The user name and password created by the user is backed up on Personal Profile Manager (PPM). The Microsoft Exchange server account is:

- Automatically created: If the user logs in on the same device for which the account is configured.
- To be manually created again: If the user logs in on another device. The following fields are prepopulated:
  - User name
  - Domain
  - Password

**Related links**

Configuring the settings file on page 39

## Supported countries

The following table lists the countries and whether they support call progress tones, DECT, and Wi-Fi. The table also lists the anti flickering frequency for camera in a specific country.

| Number | Country | Country code | Call progress tones | DECT support | Wi-Fi support | Anti-flickering frequency |
|---|---|---|---|---|---|---|
| 1 | Abu Dhabi | Abu Dhabi | ✔ | ✘ | Worldwide | 50 |
| 2 | Albania | Albania | ✔ | ✘ | ✔ | 50 |
| 3 | Argentina | Argentina | ✔ | ✔ | ✔ | 50 |
| 4 | Australia | Australia | ✔ | ✔ | ✔ | 50 |
| 5 | Austria | Austria | ✔ | ✔ | ✔ | 50 |
| 6 | Bahrain | Bahrain | ✔ | ✘ | ✔ | 50 |
| 7 | Bangladesh | Bangladesh | ✔ | ✘ | ✔ | 50 |
| 8 | Belgium | Belgium | ✔ | ✔ | ✔ | 50 |
| 9 | Bolivia | Bolivia | ✔ | ✘ | ✔ | 50 |
| 10 | Bosnia | Bosnia | ✔ | ✘ | ✔ | 50 |
| 11 | Botswana | Botswana | ✔ | ✘ | Worldwide | 50 |
| 12 | Brazil | Brazil | ✔ | ✔ | ✔ | 60 |
| 13 | Brunei | Brunei | ✔ | ✘ | ✔ | 50 |
| 14 | Bulgaria | Bulgaria | ✔ | ✔ | ✔ | 50 |
| 15 | Canada | Canada | ✔ | ✔ | ✔ | 60 |

*Table continues…*

| Number | Country | Country code | Call progress tones | DECT support | Wi-Fi support | Anti-flickering frequency |
|---|---|---|---|---|---|---|
| 16 | Chile | Chile | ✔ | ✘ | ✔ | 50 |
| 17 | China (PRC) | China | ✔ | ✘ | ✔ | 50 |
| 18 | Columbia | Columbia | ✔ | ✘ | ✔ | 60 |
| 19 | Costa Rica | Costa Rica | ✔ | ✘ | ✔ | 60 |
| 20 | Croatia | Croatia | ✔ | ✔ | ✔ | 50 |
| 21 | Cyprus | Cyprus | ✔ | ✔ | ✔ | 50 |
| 22 | Czech Republic | Czech Republic | ✔ | ✔ | ✔ | 50 |
| 23 | Denmark | Denmark | ✔ | ✔ | ✔ | 50 |
| 24 | Ecuador | Ecuador | ✔ | ✘ | ✔ | 60 |
| 25 | Egypt | Egypt | ✔ | ✘ | ✔ | 50 |
| 26 | El Salvador | El Salvador | ✔ | ✘ | ✔ | 60 |
| 27 | Finland | Finland | ✔ | ✔ | ✔ | 50 |
| 28 | France | France | ✔ | ✔ | ✔ | 50 |
| 29 | Germany | Germany | ✔ | ✔ | ✔ | 50 |
| 30 | Ghana | Ghana | ✔ | ✘ | Worldwide | 50 |
| 31 | Greece | Greece | ✔ | ✔ | ✔ | 50 |
| 32 | Guatemala | Guatemala | ✔ | ✘ | ✔ | 60 |

*Table continues…*

| Number | Country | Country code | Call progress tones | DECT support | Wi-Fi support | Anti-flickering frequency |
|---|---|---|---|---|---|---|
| 33 | Honduras | Honduras | ✔ | ✘ | ✔ | 60 |
| 34 | Hong Kong | Hong Kong | ✔ | ✔ | ✔ | 50 |
| 35 | Hungary | Hungary | ✔ | ✔ | ✔ | 50 |
| 36 | Iceland | Iceland | ✔ | ✔ | ✔ | 50 |
| 37 | India | India | ✔ | ✘ | ✔ | 50 |
| 38 | Indonesia | Indonesia | ✔ | ✘ | ✔ | 50 |
| 39 | Ireland | Ireland | ✔ | ✔ | ✔ | 50 |
| 40 | Israel | Israel | ✔ | ✔ | ✔ | 50 |
| 41 | Italy | Italy | ✔ | ✔ | ✔ | 50 |
| 42 | Japan | Japan | ✔ | ✔ | ✔ | • East Japan – Tokyo, Kawasaki, Sapporo, Yokohama, and Sendai 50Hz<br>• West Japan – 60 Hz |
| 43 | Jordan | Jordan | ✔ | ✘ | ✔ | 50 |

*Table continues…*

| Number | Country | Country code | Call progress tones | DECT support | Wi-Fi support | Anti-flickering frequency |
|---|---|---|---|---|---|---|
| 44 | Kazakhstan | Kazakhstan | ✔ | ✘ | ✔ | 50 |
| 45 | Korea | Korea | ✔ | ✘ | ✔ | • South Korea – 60 Hz<br>• North Korea – 50 / 60 Hz |
| 46 | Kuwait | Kuwait | ✔ | ✘ | ✔ | 50 |
| 47 | Lebanon | Lebanon | ✔ | ✘ | ✔ | 50 |
| 48 | Liechtenstein | Liechtenstein | ✔ | ✔ | ✔ | 50 |
| 49 | Luxembourg | Luxembourg | ✔ | ✔ | ✔ | 50 |
| 50 | Macao | Macao | ✔ | ✘ | ✔ | 50 |
| 51 | Macedonia | Macedonia | ✔ | ✘ | ✔ | 50 |
| 52 | Malaysia | Malaysia | ✔ | ✘ | ✔ | 50 |
| 53 | Mexico | Mexico | ✔ | ✔ | ✔ | 60 |
| 54 | Moldavia | Moldova | ✔ | ✘ | Worldwide | 50 |
| 55 | Morocco | Morocco | ✔ | ✘ | ✔ | 50 |
| 56 | Myanmar | Myanmar | ✔ | ✘ | Worldwide | 50 |
| 57 | Netherlands | Netherlands | ✔ | ✔ | ✔ | 50 |
| 58 | New Zealand | New Zealand | ✔ | ✘ | ✔ | 50 |

*Table continues…*

| Number | Country | Country code | Call progress tones | DECT support | Wi-Fi support | Anti-flickering frequency |
|---|---|---|---|---|---|---|
| 59 | Nicaragua | Nicaragua | ✔ | ✘ | Worldwide | 60 |
| 60 | Nigeria | Nigeria | ✔ | ✘ | Worldwide | 50 |
| 61 | Norway | Norway | ✔ | ✔ | ✔ | 50 |
| 62 | Oman | Oman | ✔ | ✘ | ✔ | 50 |
| 63 | Pakistan | Pakistan | ✔ | ✘ | ✔ | 50 |
| 64 | Panama | Panama | ✔ | ✘ | ✔ | 60 |
| 65 | Paraguay | Paraguay | ✔ | ✘ | Worldwide | 60 |
| 66 | Peru | Peru | ✔ | ✘ | ✔ | 60 |
| 67 | Philippines | Philippines | ✔ | ✘ | ✔ | 60 |
| 68 | Poland | Poland | ✔ | ✔ | ✔ | 50 |
| 69 | Portugal | Portugal | ✔ | ✔ | ✔ | 50 |
| 70 | Qatar | Qatar | ✔ | ✘ | ✔ | 50 |
| 71 | Romania | Romania | ✔ | ✔ | ✔ | 50 |
| 72 | Russia | Russia | ✔ | ✔ | ✔ | 50 |
| 73 | Saudi Arabia | Saudi Arabia | ✔ | ✔ | ✔ | 60 |
| 74 | Yugoslavia | Serbia | ✔ | ✘ | ✔ | 50 |
| 75 | Singapore | Singapore | ✔ | ✘ | ✔ | 50 |

*Table continues…*

| Number | Country | Country code | Call progress tones | DECT support | Wi-Fi support | Anti-flickering frequency |
|---|---|---|---|---|---|---|
| 76 | Slovakia | Slovakia | ✔ | ✔ | ✔ | 50 |
| 77 | Slovenia | Slovenia | ✔ | ✔ | ✔ | 50 |
| 78 | South Africa | South Africa | ✔ | ✘ | ✔ | 50 |
| 79 | Spain | Spain | ✔ | ✔ | ✔ | 50 |
| 80 | Sri Lanka | Sri Lanka | ✔ | ✘ | ✔ | 50 |
| 81 | Swaziland | Swaziland | ✔ | ✘ | Worldwide | 50 |
| 82 | Sweden | Sweden | ✔ | ✔ | ✔ | 50 |
| 83 | Switzerland | Switzerland | ✔ | ✔ | ✔ | 50 |
| 84 | Syria | Syria | ✔ | ✘ | ✔ | 50 |
| 85 | Taiwan | Taiwan | ✔ | ✔ | ✔ | 60 |
| 86 | Tanzania | Tanzania | ✔ | ✘ | Worldwide | 50 |
| 87 | Thailand | Thailand | ✔ | ✘ | ✔ | 50 |
| 88 | Turkey | Turkey | ✔ | ✘ | ✔ | 50 |
| 89 | UK | UK | ✔ | ✔ | ✔ | 50 |
| 90 | Ukraine | Ukraine | ✔ | ✘ | ✔ | 50 |
| 91 | United Arab Emirates | United Arab Emirates | ✔ | ✘ | ✔ | 50 |
| 92 | Uruguay | Uruguay | ✔ | ✘ | ✔ | 50 |

*Table continues…*

| Number | Country | Country code | Call progress tones | DECT support | Wi-Fi support | Anti-flickering frequency |
|---|---|---|---|---|---|---|
| 93 | USA | USA | ✔ | ✔ | ✔ | 60 |
| 94 | Venezuela | Venezuela | ✔ | ✘ | ✔ | 60 |
| 95 | Vietnam | Vietnam | ✔ | ✘ | ✔ | 50 |
| 96 | Yemen | Yemen | ✔ | ✘ | ✔ | 50 |
| 97 | Zimbabwe | Zimbabwe | ✔ | ✘ | ✔ | 50 |

**Related links**

Configuring the settings file on page 39

# IP Office parameters checklist

Use the following checklist if you want to manually configure the settings file for the IP Office environment:

| No. | Parameters | Set Value | ✔ |
|---|---|---|---|
| 1 | ENABLE_IPOFFICE | 1 | |
| 2 | SUBSCRIBE_LIST_NON_AVAYA | Supported string | |
| 3 | ENABLE_AVAYA_ENVIRONMENT | 0 | |
| 4 | DISCOVER_AVAYA_ENVIRONMENT | 0 | |
| 5 | ENABLE_PRESENCE | 0 | |
| 6 | PRESENCE_SERVER | Do not set | |
| 7 | CONFIG_SERVER | Do not set | |
| 8 | CONFIG_SERVER_SECURE_MODE | Do not set | |
| 9 | SIMULTANEOUS_REGISTRATIONS | 1 | |

*Table continues…*

| No. | Parameters | Set Value | ✔ |
|---|---|---|---|
| 10 | ENABLE_PPM_SOURCED_SIPPROXYSRVR | 0 | |
| 11 | ENABLE_G726 | 0 | |
| 12 | PHNEMERGNUM | Supported dial string | |
| 13 | PHNMOREEMERGNUMS | Supported dial string | |
| 14 | PSTN_VM_NUM | Supported string | |
| 15 | CONNECTION_REUSE | 1 | |

**Related links**

Configuring the settings file on page 39

# Initial setup through the device

## Navigating to the Settings screen

### Procedure

## Setting DHCP Site Specific Option Number

### About this task

Use this procedure to set the values of site-specific configuration parameters. The default value is set to 242.

### Before you begin

Ensure that you login with the administrator password to see the interface.

### Procedure

1. Go to the Settings screen.
2. Tap **More** > **DHCP Site Specific Option Number (SSON)**.
3. Enter any option between 128 to 254.

## Setting the DNS name and address

### About this task

Use this procedure to set the domain name and server address.

### Procedure

1. Go to the Settings screen.
2. Tap **More** > **DNS**.
3. Tap **DNS** > **DNS Server**.
4. Enter one or both the server addresses in the following fields:
   - **DNS Server 1**
   - **DNS Server 2**
5. Tap **DNS** > **Domain**.
6. Enter the domain name of the server.

## Setting a user group for a specific configuration

### About this task

Use this procedure for setting a group identifier to allow downloading a specific configuration set for a dedicated user group during startup. You can set group identifier between 0 to 999.

### Procedure

1. Go to the Settings screen.

2. Tap **More** > **GROUP**.
3. Enter the group identifier.

## Setting up a file server address

### About this task

Use this procedure to set up a file server address for downloading the software distribution package and settings file.

### Procedure

1. Go to the Settings screen.
2. Tap **More** > **File Server**.
3. Enter the HTTP or HTTPS address of your file server.

## Setting up an HTTP proxy and exception

### About this task

Use this procedure to specify the address of an HTTP proxy server. You can also enter the server names to bypass the proxy server.

### Before you begin

Ensure that you login with the administrator password to see the interface.

### Procedure

1. Go to the Settings screen.
2. Tap **More** > **HTTP/S Proxy Settings**.
3. Tap **Proxy host name[:port]**.
4. Enter the HTTP proxy host name with port number.
5. Tap **Bypass proxy for**.
6. Enter the server names to bypass the proxy server.

## Configuring SIP server settings

### About this task

Use this procedure to register your phone to the SIP server. You can also specify the Personal Profile Manager (PPM) server address if it is different from the SIP server address.

### Before you begin

Ensure that you login with the administrator password to see the interface.

### Procedure

1. Go to the Settings screen.
2. Tap **More** > **SIP Settings**.
3. Tap **SIP domain**.
4. Enter the server name for registration.
5. Tap **Avaya configuration server**.
6. Enter the PPM server address.
7. Tap **SIP Proxy settings**.
8. Enter the values in the following fields:
   - **SIP proxy server**: Enter the name of the SIP proxy server.
   - **Transport type**: Choose either TLS or TCP depending upon your configuration.
   - **SIP Port**: Optionally, enter 5060 for TCP or 5061 for TLS.

# Administration through the device

## Changing the date format

### Procedure

1. Go to the Settings screen.
2. Tap **SYSTEM** > **Date and time** > **Choose date format**.
3. Select the required format.
4. Tap **OK**.

## Changing to the 24–hour time format

### Procedure

1. Go to the Settings screen.
2. Tap **SYSTEM** > **Date and time**.
3. Select the **Use 24–hour format** check box.

# Enabling and disabling the wireless handset usage

## About this task

You can enable or disable the wireless handset usage only if your administrator configured the option for you.

## Procedure

1. Go to the Settings screen.
2. Perform one of the following actions:
   - To enable the wireless handset usage, tap **WIRELESS & NETWORKS** > **DECT** > **ON**.
   - To disable the wireless handset usage, tap **WIRELESS & NETWORKS** > **DECT** > **OFF**.

# Chapter 6: Backup and restore

## Back up on PPM

The Collaboration Station supports data backup by saving all non-volatile user parameters on Personal Profile Manager (PPM) in an Avaya Aura® environment. When the user logs in to any registered device, PPM restores all user data on the device.

**Note:**

You can backup and restore contacts through Avaya one-X® Portal, if your phone is registered to the IP Office server.

## Parameters backed up on PPM

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

| Parameter | Default value | Description |
|---|---|---|
| BAKLIGHTOFF | 120 | Specifies the timer to switch off the backlight of the display. |
| CLICKS | 1 | Specifies whether button click sounds are enabled. |
| CALL_PICKUP_RING_TYPE | 1 | Specifies the default call pickup ring type. |
| OUTSIDE_CALL_RING_TYPE | 1 | Specifies the default outside call ring type. |
| PRIORITY_CALL_RING_TYPE | 1 | Specifies the default priority call ring type. |
| INTERCOM_CALL_RING_TYPE | 1 | Specifies the default intercom call ring type. |
| TEAM_BUTTON_RING_TYPE_USER_SELECTION | 1 | Specifies the default team button ring type that the user selects. |
| FORWARDED_CALL_RING_TYPE | 1 | Specifies the default forwarded ring type that the user selects. |
| BRIDGED_CALL_RING_TYPE | 1 | Specifies the default bridged call ring type that the user selects. |

*Table continues…*

| Parameter | Default value | Description |
|---|---|---|
| PERSONALWAV | 1 | Specifies the user choice of the personal ring used for internal calls. |
| CALL_PICKUP_INDICATION | 3 | Specifies the following call pickup indication types:<br>• Audio<br>• Visual<br>• None |
| HEADSET_PROFILE | 0 | Specifies the headset audio profile that the user selects. |
| AMPLIFIED_HANDSET | 0 | Specifies whether the handset amplification is enabled. |
| AMPLIFIED_HANDSET_NOMINAL_LEVEL_CALL_END | 0 | Specifies whether to set the volume level in amplified mode to nominal when all calls end. |
| TIMEFORMAT | 0 | Specifies whether the time format is the am-pm format or the 24–hour format. |
| DATE_FORMAT_OPTIONS | 1 | Specifies the date display format. |
| CALL_LOG_ACTIVE | 1 | Specifies whether to activate call logging. |
| CALL_LOG_BRIDGED | 1 | Specifies whether to activate call logging for bridged calls. |
| CONTACT_NAME_DISPLAY | 1 | Specifies how contact names are displayed. |
| ENABLE_ONLINE_SEARCH | 0 | Specifies whether the default search directory is searched in the background whenever a user searches through synchronized contacts. |
| DEFAULT_CONTACTS_STORE | 1 | Specifies the account where all user contacts are added by default. |
| EXCHANGE_USER_ACCOUNT | Null | Specifies the account name for the Microsoft Exchange Server account. |
| EXCHANGE_USER_PASSWORD | Null | Specifies the user password for the Microsoft Exchange Server account. |
| ENABLE_PHONE_LOCK | 0 | Specifies whether to enable the lock screen password. |
| LOCK_SCREEN_LOCK_AFTER_TIMEOUT | 5 | Specifies the lock screen inactivity timeout in minutes. |
| SHOW_CALL_APPEARANCE_NUMBERS | 0 | Specifies whether for a user the device displays call appearance numbers in the call containers. |
| SHOW_BRIDGED_APPEARANCE_NUMBERS | 0 | Specifies whether for a user the device displays bridged appearance numbers in the call containers. |
| AUDIOPATH | 1 | Specifies whether the default audio path is speaker or headset. |
| HEADSETBIDIR | 0 | Specifies whether bidirectional signaling is supported on the headset interface. |
| LARGEFONT | 0 | Specifies whether the user selected large font size. |
| INITIAL_SCREEN | PHONE | Specifies the initial screen that the device displays when the user logs in. |

*Table continues…*

| Parameter | Default value | Description |
|---|---|---|
| BLOCK_OUTGOING_VIDEO_ANSWER_MODE | 0 | Specifies whether video is started blocked or unblocked on an incoming or escalated video call. |
| OUTGOING_CALL_MODE | 1 | Specifies the media type to be used for outgoing calls. |

# Chapter 7: Maintenance

## Device upgrade

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

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

## Device upgrade process

During boot up, the Collaboration Station performs the following tasks:

1. The Collaboration Station receives the file server address from DHCP, LLDP, or the device interface.
2. The Collaboration Station connects to the file server and searches for the upgrade file.
3. The Collaboration Station compares its software version with the version specified in the upgrade file.
4. If a newer version of the software distribution package is available, the Collaboration Station downloads the software and upgrades itself.
5. The Collaboration Station also looks for the settings file that is specified in the upgrade file and loads the settings file.

# Downloading and saving the software

### Before you begin

Ensure that your file server is set up.

### Procedure

1. Go to the Avaya Support website.
2. In the **Enter Your Product Here** field, enter `Avaya H100-Series Video Collaboration Stations`.
3. In the **Choose Release** field, click the required release number.
4. Click the **Downloads** tab.

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

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

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

### Related links

File server configuration on page 25

# Resetting a device to factory settings

### About this task

Use this procedure to reset a device to factory settings, that is, the initial state in which you received the device from the factory.

You might want to reset the device to the factory settings when you are:

- Repairing a device.
- Assigning a device to a new user by keeping the same extension but different permissions from the previous user.

Resetting a device removes the following information from the device and restores all data to the factory settings:

- All administered values
- User-specified data that includes Exchange account

- Device settings

You cannot recover the settings and data after you delete them.

### Procedure

1. Open the Settings app in the administrator mode.
2. Tap **PERSONAL** > **Device and data reset** > **DEVICE AND PERSONAL DATA** > **Factory data reset**.
3. Tap **Reset device** when the device displays the confirmation message.

# Automatic upgrade

Avaya H100-Series Video Collaboration Stations provide the facility of automatic upgrade. You can configure the settings file such that the Collaboration Stations periodically poll for a newer version of the software in the HTTP or the HTTPS server and download the files automatically.

You can set parameters in the settings files that can support following upgrade policies:

- Scheduling download for a specific time and day in a week
- Scheduling download and install on a specific date
- Setting polling interval for the new software

**Related links**

Configuration of parameters for an automatic upgrade on page 60

# Configuration of parameters for an automatic upgrade

Configure the following parameters in the settings file to set the automatic upgrade:

| Parameter | Type | Default value | Description |
|---|---|---|---|
| UPGRADE_POLICY | Integer | 2 | Specifies whether the upgrade occurs based on:<br>• Reboot only<br>• Upgrade policies only<br>• Both reboot and upgrade policies<br>Assign one of the following values:<br>• 0: Device upgrade occurs only after reboot<br>• 1: Upgrade occurs based on configured policies and management applications only |

*Table continues…*

| Parameter | Type | Default value | Description |
|---|---|---|---|
| | | | • 2: Upgrade occurs based on configured policies and after reboot<br>**Note:**<br>In an IP Office environment, the default value is set to 0 in the auto-generated settings file. |
| UPGRADE_POLLING_PERIOD | Integer | 60 | Specifies the polling interval in minutes between polling both upgrades and settings file. The range is from 0 to 10080 minutes, where the value of 0 disables polling.<br>**Note:**<br>In an IP Office environment, the default value is set to 0 in the auto-generated settings file. |
| UPGRADE_DLOAD_START | String | 00 | Specifies the start time when the device tries to download the software. To reduce the network traffic, the parameters UPGRADE_DLOAD_START and UPGRADE_DLOAD_END are used to schedule download at a time when users are out-of-office.<br>Use the following format to specify the time:<br>[Ddd]hh, where<br>• Ddd: Is a three-character string for a day of the week: Sun, Mon, Tue, Wed, Thu, Fri, and Sat<br>• hh: Is a numeric in the range of 0 to 23 for an hour of the day |
| UPGRADE_DLOAD_END | String | | Specifies the end time when the device stops trying to download the new software. Use the following format to specify the time:<br>[Ddd]hh, where<br>• Ddd: Is a three-character string for a day of the week: Sun, Mon, Tue, Wed, Thu, Fri, and Sat<br>• hh: Is a numeric in the range of 0 to 23 for an hour of the day |
| UPGRADE_INSTALL_DATE_TIME | String | | Specifies the date and time after which the new software and settings file is installed. Use the following format:<br>YYYY-MM-DDThh:mm, where<br>• YYYY: Is four numeric digits for the year<br>• MM: Is two numeric digits in the range of 00 to 12 for month<br>• DD: Is two numeric digits in the range of 1 to 31 for the day of the month<br>• T: is the time separator<br>• hh: Is two numeric digits in the range of 11 to 23 for the hour of the day |

*Table continues…*

| Parameter | Type | Default value | Description |
|---|---|---|---|
| | | | • mm: Is the two numeric digits in the range of 00 to 59 for the minutes of the hour<br><br>At the end of the installation, the device displays a confirmation message for reboot. Users can confirm or delay the reboot by half an hour. The device does not display the confirmation message if the user is in a call.<br><br>**Note:**<br><br>In an IP Office environment, the default value is set to 1970–01–01T00:00 in the auto-generated settings file. |
| DLOAD_RND_AFTER_RESET | Integer | 0 | Specifies the interval in seconds in which the downloading attempts randomizes after the device reboots. The range is from 0 to 32767 seconds. |
| DLOAD_RND | Integer | 3600 | Specifies the interval in seconds in which the downloading attempts randomizes during background downloads. The range is from 0 to 32767 seconds. |

**Related links**

Automatic upgrade on page 60

# Manual upgrade

## Upgrading a device through System Manager

### About this task

Use the following procedure to perform bulk upgrade of Collaboration Station.

### Before you begin

Ensure that you have the latest version of the software on the file server.

### Procedure

1. In the System Manager interface, provide the range of the Collaboration Station registrations that require an upgrade.
2. Press **Reboot**.

   As part of the boot up process, the Collaboration Station downloads the upgrade file from the file server. The Collaboration Station then compares the current version of the build with the one in the upgrade file. If the upgrade file has a higher version, the device reads the upgrade file further and downloads the higher version of the build.

# Upgrading a device through the Settings app

## About this task

You can use the update option or reboot the device to upgrade it. With the update option, the device immediately downloads and installs the software if an updated version is available. With rebooting, the device might upgrade immediately or later based on the upgrade policy configured for the device

## Before you begin

Ensure that you have the latest version of the software on the file server. .

## Procedure

- To upgrade the device using the update option:
  1. Open the settings app in the admin mode.
  2. Tap **SYSTEM** > **About** > **Software information** > **Update now**.

     If the device already has the latest version, the device displays a device up-to-date message and does not upgrade.
- To upgrade the device by rebooting:
  1. Go the Settings screen.
  2. Tap **PERSONAL** > **Device and data reset** > **DEVICE** > **Reboot**.
  3. Tap **OK** for confirmation.

# Chapter 8: Troubleshooting

## Error message “Not enough power to activate the device”

### Condition

The device displays the message “Not enough power to activate device. Please contact your administrator.”

### Cause

There is not enough power coming from PoE port for the device to operate properly.

### Solution

Perform one of the following actions:

- Supply the AC power to the device by connecting the power adapter to an electrical outlet.
- In the settings file, set the ASSUME_SP_POE parameter to 1 so that the device operates in low power mode by disabling some of the USB ports.
- Connect the PoE injector and in the settings app, select the **Single port PoE injector connected** check box under **Network** > **Ethernet** > **Power over Ethernet (PoE)**.

## Camera not working

### Camera not working

Camera is not capturing video images or the camera LED is not lighting up.

### Camera cable not connected properly

Camera has a dedicated USB in the Collaboration Station and works only if the camera cable is connected to the dedicated USB.

### Solution

Ensure that the camera cable is connected to the dedicated camera USB in the Collaboration Station and you have opened the privacy shutter of the camera.

# The base of the device is hot

### Condition

The base of the device is hot.

### Cause

Avaya H175 Video Collaboration Stations generate more heat than other deskphones. This behavior is expected and within product safety standards (IEC 60950-1). The heat from the deskphone dissipates from the lower plastic cover and finally through the space between the rubber foot pads.

### Solution

Ensure that:

- You have put the device on a flat surface, such as a table, for proper heat dissipation.
- You have not kept any object, such as paper or cloth, below the device.
- The operating temperature is between 0 °C to 40 °C as the surface temperature increases relative to the operating temperature. The operating temperature is the ambient temperature of the room.

# Video calls fail post installation

### Condition

Post installation, the user is unable to start a video call or receive an incoming video call.

### Cause

Inappropriate configuration of a Session Border Controller rule that might cause video call types to fail.

### Solution

If connecting through Session Border Controller (SBC), ensure that for the SBC media rule, you enabled SRTP in the video encryption type. The Collaboration Station requires both audio and video to be SRTP encrypted.

# Firmware got corrupted

### Condition

The firmware got corrupted and you want to restore the firmware to its original state.

The firmware corruption can occur due to power outage during the device upgrade time or a corrupt system file.

### Solution

You can use the boot recovery procedure to clear the device and restore the Collaboration Station to factory settings. You can use the boot recovery procedure only if you have not changed the default password.

1. Reboot the device.
2. Press and hold the star key (*) on the dialpad when you see the message `Avaya The Power of We` on screen.
3. Release the key after 5 seconds.
4. The Collaboration Station displays the Android system recovery screen after approximately 30 seconds.
5. Press **1** to start the boot recovery procedure.
6. Enter the admin password when the Collaboration Station prompts you.

   The Collaboration Station starts the boot recovery procedure and displays a list of options.
7. Select one of the following options:
   - **Reboot**: Stops the boot recovery procedure and reboots the deskphone.
   - **CLEAR Phone** : Performs resetting of the deskphone to factory settings.
   - **Erase /cache**: Erases the cache partition of the deskphone that is primarily used to store recovery logs and temporary files.
   - **Erase /var**: Erases the var partition of the deskphone that is primarily used for storing device logs.
   - **Wipe cache and var**: Clears both cache and var partitions of the deskphone.
   - **Wipe /data**: Erases the data partition of the deskphone that is primarily used to store system and application databases.
   - **Wipe /vendor**: Clears the vendor partition of the deskphone.
   - **Clear OPKGs**: Deletes the downloaded OPKG file from the device. OPKG packages are the tar files download by an administrator.
   - **Swap banks and reboot**: Swaps the boot banks on the device that results in primary boot bank becoming secondary boot bank and vice versa. The deskphone always has 2 copies of firmwares:
     - Current firmware. The deskphone uses this firmware to boot up.
     - Previously installed firmware. This firmware is updated each time the firmware on the deskphone is upgraded.

     For example, if the deskphone is running build 1000 and the deskphone is upgraded to build 2000, the primary boot bank will contain the build 2000 and the secondary backup boot bank will contain the build 1000.

# Chapter 9: System Failover and Survivability

## Configuring survivability for H175 Collaboration Stations

By administering survivability configuration parameters using the `H1xxsettings.txt` file (or using the default values if applicable), the SIP deskphones can quickly switch to an active controlling server and experience minimal disruption. You can also configure survivability between the following servers:

- Avaya Aura® and IP Office, if IP Office is configured in the branch mode.
- IP Office and IP Office, if configured as primary and secondary.

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

The parameters are configured for Avaya Aura® environment.

The failover/failback parameters are:

- CONTROLLER_SEARCH_INTERVAL: The time the phone waits to complete the maintenance check for Monitored Controllers.
- DISCOVER_AVAYA_ENVIRONMENT: Determines whether the phone operates in a mode to comply with the Avaya environment mode (provision of SIP/AST features and use of PPM for download and backup/restore).
- ENABLE_REMOVE_PSTN_ACCESS_PREFIX: Enables the removal of the PSTN access prefix from collected dial strings when the phone is communicating with a non-AST controller.
- FAILBACK_POLICY: Failback Policy.
- FAST_RESPONSE_TIMEOUT: Fast Response Timer.
- PSTN_VM_NUM: The number called when the phone is in failover and the Message button is pressed.

  **Note:**

  This parameter is only available for IP Office.
- RECOVERYREGISTERWAIT: Reactive Monitoring Interval in seconds.
- REGISTERWAIT: Proactive Monitoring Interval in seconds.
- SIP_CONTROLLER_LIST: Configured Controller list. A comma-separated list of SIP URIs, a hostname, or numeric IP address. If null, DHCP/DNS will provide the defaults.

- SIMULTANEOUS_REGISTRATIONS: The number of Session Managers with which the deskphone will simultaneously register.
- SIPREGPROXYPOLICY: Registration Policy. The default value of this parameter is simultaneous.

**Related links**

Configuring survivability through the phone interface on page 68

## Configuring survivability through the phone interface

### About this task

Use the following procedure to configure SIP domain and controller.

### Before you begin

Ensure that you have SIP domain name and SIP proxy settings.

### Procedure

1. Navigate to the **Settings** > **More** > **SIP Settings** .
2. Login with your administrator credentials.
3. Enter **SIP Domain** and **SIP Proxy Settings**.

**Related links**

Configuring survivability for H175 Collaboration Stations on page 67

# Supported operations

During failover and survivability, the following operations are valid through the phone:

- Making a call (includes emergency calls).
- Receiving a call.
- Call transfer.
- Mid call features: Call hold and mute.
- Audio Conference: Local three-way audio conference.

# Index

## T



## U



## V



## W