Installing and Administering Avaya Vantage™ in an Avaya Aura® or IP Office Environment

Release 2.2
Issue 5
May 2021

© 2017-2021, Avaya Inc.
All Rights Reserved.

Note

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

Shrinkwrap License (SR). End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Regulatory Statements

Australia Statements

Handset Magnets Statement:

Danger:

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

Industry Canada (IC) Statements

RSS Standards Statement

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

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

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

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

Radio Transmitter Statement

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

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

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

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

Radiation Exposure Statement

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

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

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

Japan Statements

Class B Statement

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

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

Denan Power Cord Statement

Danger:

Please be careful of the following while installing the equipment:

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

警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

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

México Statement

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

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

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

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

Brazil Statement

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

Power over Ethernet (PoE) Statement

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

Taiwan Statements

低功率電波輻射性電機管理辦法

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

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

前項合法通信，指依電信法規定作業之無線電通信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

U.S. Federal Communications Commission (FCC) Statements

Compliance Statement

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

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

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

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

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

WiFi and BT transmitter

- Frequencies for 2412-2472 MHz, transmit power: 19.84 dBm
- Frequencies for 5180-5240 MHz, transmit power: 22.5 dBm

General Safety Warning

- Use only the Avaya approved Limited Power Source power supplies specified for this product.
- Ensure that you:
  - Do not operate the device near water.
  - Do not use the device during a lightning storm.
  - Do not report a gas leak while in the vicinity of the leak.
  - For Accessory Power Supply - Use Only Limited Power Supply Delta Electronics Inc. Model: ADP-30HR B, output: 48Vdc, 0.66A.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

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

Android, Google and Google Play are trademarks of Google Inc.

Device Usage Consent

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

Contents

Chapter 1: Introduction ... 12
Purpose ... 12
Change history ... 12
Chapter 2: Avaya Vantage™ overview ... 16
Optional components for the Avaya Vantage™ device ... 16
New in this release ... 17
Chapter 3: Initial setup and connectivity ... 20
Initial setup checklist ... 20
Software and hardware requirements ... 21
Avaya Aura® configuration for Avaya Vantage™ ... 23
IP Office configuration for Avaya Vantage™ ... 25
Deployment comparison between Avaya Aura® and IP Office ... 26
Avaya Session Border Controller for Enterprise configuration ... 28
Avaya Vantage™ deployment through Device Enrollment Services ... 29
Avaya Vantage™ firmware in Device Enrollment Services ... 29
Configuration for Device Enrollment Services discovery ... 30
Identity certificate generation in Device Enrollment Services ... 30
Preinstallation data ... 31
System Manager user profile worksheet ... 31
IP Office SIP user and extension settings ... 32
DHCP settings worksheet ... 32
Settings file worksheet ... 33
DHCP server setup ... 36
Setting up a DHCP server ... 36
File server setup ... 36
Setting up a file server ... 38
Downloading device firmware ... 39
Configuring parameters in the settings file ... 39
SNTP server setup ... 40
IP address configuration ... 41
Parameter configuration to support IPv6 operation ... 42
Configuring IPv4 through the Settings menu ... 47
Configuring IPv6 through the Settings menu ... 47
Power and network connectivity ... 48
Power management ... 48
Connecting the Avaya Vantage™ device to the network ... 49
Installation wizard considerations ... 50
Setting up K165 or K175 using the Android installation wizard ... 50
Installing the K155 wireless module ... 52

Configuring Wi-Fi from the Settings menu ... 53
Handset connection to Avaya Vantage™ ... 54
Connecting the handset cradle to Avaya Vantage™ ... 54
Connecting a wired handset ... 55
Connecting a wireless handset ... 56
Removing the pairing with the wireless handset ... 57
Wall mounting options for Avaya Vantage™ ... 57
Mounting Avaya Vantage™ directly on a wall ... 58
Mounting Avaya Vantage™ on a wall plate ... 59
Wall mounting Avaya Vantage™ along with a handset cradle ... 62
Chapter 4: Security configuration ... 65
Security best practices ... 67
Access control and user privacy ... 68
Password security policies ... 69
Administrator password configuration ... 70
Certificate management ... 71
Certificate usage by applications ... 73
Generating a PKCS12 file with a friendly name ... 75
Adding a friendly name to an existing PKCS12 file ... 76
Guidelines for using a self-signed certificate ... 76
Use of Avaya product certificates ... 77
Obtaining the Avaya SIP Product CA certificate ... 77
Obtaining the Avaya Aura® System Manager CA certificate ... 78
Device Enrollment Services for secure redirection to the file server ... 78
Time synchronization ... 79
SSH access control ... 79
Android Debug Bridge configuration ... 80
Enabling or disabling ADB through the Settings menu ... 80
VLAN separation ... 81
VLAN configuration parameters ... 81
Settings menu access control ... 82
FIPS mode ... 83
FIPS mode configuration ... 84
Disabling FIPS mode from the Settings menu ... 85
Android security patches ... 86
Parameter configuration for secure installation ... 86
Chapter 5: Data privacy controls on Avaya Vantage™ and Avaya Vantage™ Connect ... 90
Avaya Vantage™ data privacy controls ... 91
Data categories containing personal data ... 91
User information storage ... 91
Personal data human access controls ... 92
Personal data programmatic or API access controls ... 93
Encryption controls for personal data “at rest” ... 93

Encryption controls for personal data “in transit” 93
Personal data retention periods..... 94
Personal data export controls..... 94
Personal data pseudonymization..... 95
Avaya Vantage™ Connect data privacy controls..... 95
Data categories containing personal data..... 95
User information storage..... 96
Personal data human access controls..... 96
Personal data programmatic or API access controls..... 97
Encryption controls for personal data “at rest”..... 97
Encryption controls for personal data “in transit” 98
Personal data retention periods..... 98
Personal data export controls..... 99
Personal data pseudonymization..... 99
Chapter 6: Device configuration..... 100
Configuration priority for the CSDK-based telephony application..... 101
Device configuration using LLDP..... 101
Initial values of parameters transmitting in LLDP frames 102
TLV impact on system parameter values..... 103
Device configuration using DHCP options..... 106
Configurable DHCP options..... 106
DHCP site-specific options..... 109
Device configuration using a 46xxsettings.txt settings file..... 111
Customization of the settings file..... 112
User group configuration in the settings file..... 114
Configuring parameters in the settings file..... 115
Device configuration using Avaya Aura® Device Services..... 115
Device configuration using the Settings menu on the device..... 116
Device configuration checklist..... 116
Enabling administrator settings on the device..... 118
Configuring the file server address through the Settings menu..... 119
Setting the DNS name and address..... 119
Setting the Avaya Aura® Device Services server address..... 120
Setting a user group for a specific configuration..... 121
Setting up an HTTP proxy and exception..... 121
Configuring SIP server settings..... 122
Setting up a DHCP site-specific option number..... 123
Additional network configuration..... 123
Verifying device configuration..... 125
Chapter 7: Application setup..... 127
Pushing applications onto the Avaya Vantage™ device..... 128
Push command examples..... 129
Uninstalling a pushed application..... 129

Avaya telephony applications supported on Avaya Vantage™ 130
Setting up an Avaya™ Client SDK application as the active telephony application..... 130
ACTIVE_CSDK_BASED_PHONE_APP parameter usage..... 131
Package names of Avaya™ Client SDK applications..... 132
Access to Google Play applications for K165 and K175..... 132
Access to applications from unknown sources..... 133
Application download control through an XML-based configuration file..... 133
Editing a black or white list..... 134
Chapter 8: Emergency call configuration..... 136
Parameters for emergency numbers..... 136
Chapter 9: Directory search configuration..... 138
Directory search and contact functionality comparison..... 138
Avaya Aura® contact management..... 139
IP Office contact search options..... 139
LDAP directory search..... 139
Chapter 10: Kiosk mode configuration..... 141
Kiosk mode configuration checklist..... 141
Applications to pin in Kiosk mode..... 142
Unpinning applications in Kiosk mode..... 143
Starting Kiosk mode for the first time..... 143
Exiting the Kiosk mode..... 144
Chapter 11: Device start up, screen saver, and lock configuration..... 145
Device start-up configuration..... 145
Login screen configuration..... 145
Screen saver configuration..... 146
Parameters for screen saver configuration..... 146
Lock screen and idle time configuration..... 148
Chapter 12: Avaya Vantage™ Connect configuration..... 149
Hot dialing configuration..... 149
Hot dialing configuration checklist..... 149
Parameter configuration example for hot dialing..... 151
Microsoft Exchange Calendar integration with Avaya Vantage™ Connect..... 152
Parameters for calendar configuration..... 152
Avaya Connect Expansion Module configuration..... 153
Feature buttons supported by Avaya Connect Expansion Module..... 154
Expansion Module configuration checklist..... 155
Adding a feature button to the SIP endpoint through System Manager..... 157
Adding a feature button to the SIP endpoint through IP Office Web Manager..... 159
Chapter 13: Maintenance..... 161
Restoring factory settings from the Settings menu..... 161
Clearing user data stored in PPM..... 162
Rebooting Avaya Vantage™ from the Settings menu..... 162

Failover and survivability.... 163
Debugging and monitoring options.... 163
Enabling verbose logging.... 163
Generating a debug report.... 164
Generating an audio report.... 166
Copying debug report from internal flash memory.... 168
Opening a debug or audio report.... 168
Configuring the SSH server settings.... 169
Enabling port mirroring.... 170
Pinging a device on the network.... 170
SLA Mon™ for diagnostics.... 171
Chapter 14: Device upgrade.... 172
Device upgrade process.... 172
Firmware upgrade prerequisites.... 173
Parameters for defining upgrade policy.... 174
Automatic upgrades.... 177
Scenario: Performing a scheduled upgrade.... 177
Upgrading Avaya Vantage™ using the Update option.... 178
Upgrading Avaya Vantage™ using System Manager.... 178
Upgrading Avaya Vantage™ using IP Office.... 179
Support for two or more software versions on the same file server path.... 180
Two different file servers or directories.... 180
K1xxSupgrade.txt to point to two different software versions.... 181
46xxsettings.txt to point to two different software versions.... 182
CSDK-based application upgrades.... 183
Enabling a wireless handset upgrade.... 183
Chapter 15: Troubleshooting.... 184
Firmware is corrupted.... 184
Software distribution packages cannot be uploaded using the Utility Server.... 185
Video is not available.... 186
Video remains stuck after it is resumed.... 186
Screen lock is enabled but the swipe to unlock action does not prompt for the password.... 186
The device displays a security certificate error.... 187
H.323 contacts are downloaded without a phone number.... 188
Some applications do not support Android 8.1.... 188
Some applications are not downgrading on K175 with Android 8.1.... 189
Call is stuck after the port switch is set to forceUnauthorized.... 189
Cannot join a conference bridge when DTMF is set to in-band.... 190
Cannot find application package names for Kiosk mode.... 190
Chapter 16: Resources.... 191
Documentation.... 191
Finding documents on the Avaya Support website.... 192
Avaya Documentation Portal navigation.... 193

Training.... 194
Viewing Avaya Mentor videos.... 194
Support.... 195
Using the Avaya InSite Knowledge Base.... 195
Appendix A: Supported configuration parameters.... 196
Parameters for controlling configuration parameter downloads.... 196
Phone parameters.... 197
General phone functionality settings.... 198
Device UI related settings.... 201
Server addresses and ports.... 213
SIP user-level settings.... 224
Server environment settings.... 225
Network settings.... 226
General settings.... 227
Ethernet interface settings.... 236
VLAN settings.... 238
IEEE 802.1X settings.... 241
Active phone application.... 243
Application settings.... 244
Avaya™ Client SDK application parameters.... 246
Avaya Vantage™ Connect parameters.... 261
IP Office parameters.... 272
Upgrade-related parameters.... 275
Protocol-specific parameters.... 280
Security parameters.... 281
Certificate configuration parameters.... 281
SELinux settings.... 288
FIPS mode parameter.... 289
General account IDs & passwords.... 289
Login screen specific parameters.... 293
Device lock and idle time parameters.... 294
Parameters to lock and obscure Settings menu options.... 296
Emergency call settings.... 298
Logging and debugging parameters.... 300
SLA Mon™ agent settings.... 306
USB parameters.... 307
LDAP directory service settings.... 308
Accessibility settings.... 311
Online help URL setting.... 312
Appendix B: Parameter configuration examples in the settings file.... 313
Parameter configuration example for Avaya Aura® with SIP credentials.... 313
Parameter configuration example for Avaya Aura® with user enterprise credentials.... 314
Parameter configuration example for IP Office with SIP credentials.... 314

Chapter 1: Introduction

Purpose

This document provides checklists and procedures for installing, configuring, administering, and troubleshooting Avaya Vantage™ in an Avaya Aura® or IP Office environment. This document is primarily intended for implementation engineers and administrators.

This document does not cover Open SIP deployments. For information about deploying Avaya Vantage™ in an Open SIP environment, see *Installing and Administering Avaya Vantage™ in an Open SIP Environment*.

Change history

Issue	Date	Summary of changes
Release 2.2, Issue 5	May 2021	• Updated about the location from where to download the Kiosk application APK file in Kiosk mode configuration checklist on page 141.
Release 2.2, Issue 4	September 2020	• Updated Guidelines for using a self-signed certificate on page 76. • Updated DHCP site-specific options on page 109. • Updated Parameters for emergency numbers on page 136. • Added a new chapter, “Device start-up, screen saver, and lock configuration”. • Updated Expansion Module configuration checklist on page 155. • Updated Adding a feature button to the SIP endpoint through System Manager on page 157. • Added Example: Administering call pickup on page 158. • Updated Adding a feature button to the SIP endpoint through IP Office Web Manager on page 159. • Removed the chapter about Avaya Connect Transcribe configuration.

Table continues…

Issue	Date	Summary of changes
		• Updated the following parameter descriptions in Appendix A: ADMIN_INITIAL_SCREEN, BRANDING_VOLUME, and BAKLIGHTOFF. • Added the following parameter descriptions in Appendix A: - BACKLIGHT_SELECTABLE - DARK_BOOTUP - DIRUSERNAME - DIRPASSWORD - DIRSTARTTLS - PRESERVE_LOGIN_PASSWORD - ENABLE_PUBLISH_MAC_ADDRESS - SCREENSAVER_IMAGE - SCREENSAVER_IMAGE_DISPLAY - SCREENSAVER_IMAGE_SELECTABLE - SHOW_LAST_EXTENSION
Release 2.2, Issue 3	April 2020	• Updated enrollment code information in Configuration for Device Enrollment Services discovery on page 30. • Updated certificate generation information in Identity certificate generation in Device Enrollment Services on page 30. • Updated time retrieval information in SNTP server setup on page 40. • Removed information about dual adapter splitter usage. • Added wall mounting instructions in the sections under Wall mounting options for Avaya Vantage on page 57. • Updated the sections under Avaya Connect Expansion Module configuration on page 153 with information about support of Avaya Connect Expansion Module in an IP Office Manager environment. • Added Support for two or more software versions on the same file server path on page 180. • Added Enabling a wireless handset upgrade on page 183. • Updated the TLS_VERSION parameter information in Protocol-specific parameters on page 280. • Removed references of the CERT_INSTALL_APPLICATION_LIST parameter from the lists of supported parameters.

Table continues…

Issue	Date	Summary of changes
		• Updated the EWSSSO parameter information in Avaya Client SDK application parameters on page 246. • Added Presence settings parameters on page 271. • Added ENABLE_IPO_CALL_LOG in IP Office parameters on page 272.
Release 2.2, Issue 2	February 2020	• Updated PPM configuration on page 23. • Updated Deployment comparison between Avaya Aura and IP Office on page 26. • Added Security best practices on page 67. • Added Guidelines for using a self-signed certificate on page 76. • Updated FIPS mode on page 83 and FIPS mode configuration on page 84. • Added Disabling FIPS mode from the Settings menu on page 85. • Added Android security patches on page 86. • Updated Directory search and contact functionality comparison on page 138. • Updated Avaya Aura contact management on page 139. • Updated the list of application package names in Applications to pin in Kiosk mode on page 142. • Updated the following parameter descriptions in Appendix A: ENABLE_USB_GENERAL_PURPOSE, HTTPDIR, TLSDIR, and FILE_SERVER_URL. • Added a parameter description for ENABLE_SIP_USER_ID. • Removed AUDIO_DEVICE_CALL_CONTROL_ENABLED in Avaya Vantage Connect parameters on page 261.
Release 2.2, Issue 1	October 2019	• Moved Specifications information to *Using the Avaya Vantage™ Device*. This information has been removed from this document. • Updated New in this release on page 17. • Updated Avaya Aura System Manager configuration on page 23. • Updated PPM configuration on page 23. • Added Configurations to support video calls on Avaya Vantage on page 24. • Updated the sections under Avaya Vantage deployment through Device Enrollment Services on page 29. • Added IP address configuration on page 41.

Table continues…

Issue	Date	Summary of changes
		• Added Parameter configuration to support IPv6 operation on page 42. • Added Configuring IPv4 through the Settings menu on page 47. • Added Configuring IPv6 through the Settings menu on page 47. • Added FIPS mode on page 83. • Updated Configuring the file server address through the Settings menu on page 119. • Updated Setting the DNS name and address on page 119. • Updated Verifying device configuration on page 125. • Updated Package names of Avaya Client SDK applications on page 132. • Updated Applications to pin in Kiosk mode on page 142 with additional package examples. • Updated the steps in Unpinning applications in Kiosk mode on page 143. • Added a new step in Exiting the Kiosk mode on page 144. • Added a new chapter: Avaya Connect Expansion Module configuration on page 153. • Added a new chapter: Hot dialing configuration on page 149. • Added a new chapter: Microsoft Exchange Calendar integration with Avaya Vantage Connect on page 152. • Updated Device upgrade on page 172. • Added new troubleshooting sections: - The device displays a security certificate error on page 187 - H.323 contacts are downloaded without a phone number on page 188 - Call is stuck after the port switch is set to forceUnauthorized on page 189 - Cannot join a conference bridge when DTMF is set to in-band on page 190 • Added new parameters and updated parameter descriptions throughout Appendix A. • Rebranded Avaya Equinox® to Avaya IX™ Workplace Client and Avaya Breeze® Client SDK to Avaya™ Client SDK. These changes take effect with Avaya IX™ Workplace Client, previously known as Avaya Equinox®, Release 3.7.

Chapter 2: Avaya Vantage™ overview

The Avaya Vantage™ device combines the advantages of a customizable unified communications solution and a fully functional Android device. Avaya Vantage™ supports all Android 8.1 accessibility services, including talk-back, magnification, and font or display size configuration. You can use Avaya™ Client SDK and custom applications to integrate communications into business processes using your Avaya Vantage™ device.

According to your business needs, you can choose from the following Avaya Vantage™ device variants:

- Avaya Vantage™ K175: Standard device with an 8-inch screen and an integrated camera for full access to video calls and conferences. You can cover the camera using a mechanical camera shutter.
- Avaya Vantage™ K165: Standard device with an 8-inch screen that does not include an integrated camera. You can still receive video from other users.
- Avaya Vantage™ K155: Device with a small 5-inch screen. The device also includes a physical keypad and an integrated camera, but it does not include a mechanical camera shutter.

Avaya Vantage™ works with Avaya Aura®, IP Office, and Open SIP environments.

Avaya Vantage™ supports the following Avaya™ Client SDK-based telephony applications:

- Avaya Vantage™ Connect
- Avaya IX™ Workplace Client

  Avaya IX™ Workplace Client on Avaya Vantage™ only supports Avaya Aura® and IP Office. Open SIP deployments are not supported.

Optional components for the Avaya Vantage™ device

You can use the following optional components with the Avaya Vantage™ device:

- J1B1 wired handset and cradle kit
- J2B1 wireless handset and cradle kit
- Replacement handset cord
- AC power adapter (international)
- AC power cord for regions

- Wireless module for K155

You must order these optional components separately.

New in this release

Avaya Vantage™ Release 2.2 Service Packs include the following new and enhanced functionalities:

Device MAC address publishing support

You can use the ENABLE_PUBLISH_MAC_ADDRESS parameter to enable device MAC address publishing in all SIP signaling. When you enable this option, a third-party location service can use the device MAC address to determine and report the location of the device for emergency calls.

Device start-up enhancement

As an administrator, you can now minimize audio and visual notifications when Avaya Vantage™ turns on or restarts through configuration parameters.

Preserve login credentials

As an administrator, you can now control whether to preserve login credentials on the Avaya Vantage™ Login screen after you log out or tap **Cancel** during a login operation. You can control this behavior through configuration parameters.

Screen saver management

As an administrator, you can now centrally manage screen saver behavior on Avaya Vantage™ devices through configuration parameters. You can push screen saver images to Avaya Vantage™ and choose a default screen saver image for the device. You can also control whether the device users can set up a screen saver of their choice locally from the device.

Call pickup alert support

In an Avaya Aura® environment, Avaya Vantage™ Connect supports audio and visual alerts for call pickup on the pickup group members' device when a member of the group receives a call. An administrator can enable or disable these call pickup alerts.

Contact search support using PPM

Avaya Vantage™ Connect now supports enterprise contact search when using PPM.

Arabic language support

Avaya Vantage™, Avaya Vantage™ Connect, and Avaya Connect Expansion Module support Arabic.

Avaya Connect Expansion Module support in an IP Office environment

The Expansion Module application is supported in an Avaya Aura® or IP Office environment.

Presence support

Avaya Vantage™ Connect supports the Presence feature in an Avaya Aura® or IP Office environment.

Device Enrollment Services enrollment code options

Device Enrollment Services supports an 8-digit or 12-digit enrollment code. The 8-digit code is the most secure. The numbers in this code are randomly generated and it has an expiry date. The 12-digit enrollment code consists of the account ID and a 4-digit PIN. The 12-digit code is easy to remember and does not expire.

Time retrieval support from network sources

If the configured or default SNTP servers are not accessible, Avaya Vantage™ can now retrieve time from HTTP or HTTPS services that the device accesses before the SIP registration. The following are the services that the devices accesses in order:

- Device Enrollment Services.
- HTTP or HTTPS file server for configuration and software file download.
- Avaya Aura® Device Services when USER_AUTH_FILE_SERVER_URL is configured.
- PPM.

Wireless handset automatic upgrade support

You can use the ENABLE_CORDLESS_HANDSET_UPDATE parameter to enable an automatic upgrade of the wireless handset paired with Avaya Vantage™.

Parameter modifications

Several parameter definitions have changed. Some parameters support new values, and some have new default values.

For example, the default value of TLS_VERSION is now 1, which permits only TLS 1.2. If any services do not support TLS 1.2, you must upgrade them to support TLS 1.2. Otherwise, you can change the value of TLS_VERSION to 0 to allow TLS 1.0.

For more information about Avaya Vantage™ parameters, see:

- *Installing and Administering Avaya Vantage™ in an Avaya Aura® or IP Office Environment*
- *Installing and Administering Avaya Vantage™ in an Open SIP Environment*

Release 2.2

Avaya Vantage™ Release 2.2 introduces the following:

Call control on headsets

You can use the call control capabilities on various USB and Bluetooth headset or speakerphone models with Avaya Vantage™. This functionality is supported with Avaya Vantage™ Connect Release 2.2 and Avaya IX™ Workplace Client Release 3.7.

Hot dial support

You can configure hot dialing on Avaya Vantage™ Connect if you want the application to automatically dial a specific phone number. When the hot dial feature is enabled, the application automatically calls the configured phone number when the device is off-hook. For example, if you lift the handset, then Avaya Vantage™ Connect will automatically call the configured number.

Avaya Connect Expansion Module

The Avaya Connect Expansion Module application features a large display to extend the number of call feature buttons for Avaya Vantage™ Connect. The Avaya Connect Expansion Module application can be integrated with Avaya Vantage™ Connect in an Avaya Aura® environment.

Bridge Line Appearance support

You can use Bridged Line Appearance (BLA) in Avaya Vantage™ Connect directly or through Avaya Connect Expansion Module. BLA typically involves a boss-secretary scenario, where the primary number belongs to the boss. When someone calls the boss, either the boss or secretary can answer the call. If the secretary answers the call first, the boss can bridge onto the call. Avaya Vantage™ Connect supports BLA only in an Avaya Aura® environment.

Calendar support

Avaya Vantage™ Connect supports calendar integration with Microsoft Exchange Server. When the calendar is enabled, you can see your meetings in the Calendar tab on Avaya Vantage™ Connect.

IPv6 support

Avaya Vantage™ and the active Avaya™ Client SDK application on Avaya Vantage™ can now work and internetwork in IPv4 and IPv6 mode. Currently Avaya Vantage™ supports IPv6 only in an Avaya Aura® environment. IPv6 support is not available in an IP Office or Open SIP environment.

Quick Lock in Kiosk device

When using Avaya Vantage™ as a Kiosk device, you can use Quick Lock to define and use a simple password for locking and unlocking your device.

Avaya Equinox® and Client SDK rebranding

In Release 3.7, Avaya Equinox® is being rebranded to Avaya IX™ Workplace Client. Avaya Breeze® Client SDK is also being rebranded to Avaya™ Client SDK. Avaya Vantage™ Release 2.2 will interoperate with Avaya IX™ Workplace Client Release 3.7. The Avaya Vantage™ customer documentation is being updated with these new names.

Chapter 3: Initial setup and connectivity

Initial setup checklist

The following checklist describes tasks that you must perform to set up your Avaya Vantage™ device.

No.	Task	Notes	✔
1	Determine whether you are setting up the device in an environment with Device Enrollment Services.	You can install Avaya Vantage™ in the following ways: • With the Device Enrollment Services discovery process: The installation process begins after the phone is connected to a network. This is an automated process. For more information about installation with Device Enrollment Services, see Avaya Vantage deployment through Device Enrollment Services on page 29. • Without the Device Enrollment Services discovery process: The installation process includes a series of manual preconfiguration tasks as mentioned in this checklist.	
2	Review prerequisite information.	If you do not have all required software and hardware, Avaya Vantage™ might not function as expected. See Software and hardware requirements on page 21.	
3	Gather preinstallation data.	Preinstallation data is required to perform initial parameter setup and to create user accounts for Avaya Vantage™.	
4	Set up a DHCP server.	See DHCP server setup on page 36. This task is also applicable in a Device Enrollment Services environment.	

Table continues…

No.	Task	Notes	✔
5	Set up a file server.	See File server setup on page 36. This task does not apply in a Device Enrollment Services environment.	
6	Obtain the device firmware and `46xxsettings.txt` file, and save them on the file server.	See Downloading device firmware on page 39. For information about configuring parameters in the settings file, see Configuring parameters in the settings file on page 39. This task does not apply in a Device Enrollment Services environment. However, you need a settings file if the provisioning URL in Device Enrollment Services is set to `https://des.avaya.com`. For more information, see “Profile management” in *Using Avaya Device Enrollment Services to Manage Endpoints*.	
7	Configure SNTP servers.	Ensure that an SNTP server is reachable from the network where you are installing Avaya Vantage™ and the SNTPSRVR value is set with the SNTP server address. See SNTP server setup on page 40. This task is also applicable in a Device Enrollment Services environment.	
8	Connect Avaya Vantage™ to your network and, if required, to a power supply.	Connection to a power adapter is only required in certain conditions. For more information, see Power and network connectivity on page 48.	
9	(Optional) Install the wireless module on the K155 device.	For Wi-Fi and Bluetooth connectivity on the K155 device, install the wireless module on the device. On K165 and K175, the wireless capability is built-in. See Installing the K155 wireless module on page 52.	
10	(Optional) Connect a handset.	This step is required only if you want to use a handset with Avaya Vantage™. See Handset connection to Avaya Vantage on page 54.	

Software and hardware requirements

Ensure that you have the following before you install Avaya Vantage™.

Components and other software requirements

The following components must be installed and configured on your network. For more information about supported product releases, see Avaya Compatibility Matrix.

- Avaya Aura® or IP Office server components. You can deploy Avaya Vantage™ with one of the following:
  - The latest Avaya Aura® Release 6.3 Service Pack or a higher release.
  - IP Office Release 11.0 or later.

    IP Office 11.0.4 or later supports Avaya IX™ Workplace Client on Avaya Vantage™ K165 and K175. Earlier IP Office releases do not support Avaya IX™ Workplace Client on Avaya Vantage™.
- A DHCP server for providing dynamic IP addresses.

  In an environment without Device Enrollment Services, the DHCP server also provides the address details of the file server that the device uses.
- A file server for downloading software distribution packages and the settings files that contain the device configuration.

  You can use an external HTTP or HTTPS file server. In the Avaya Aura® environment, you can use the Utility Server, which is embedded in Avaya Aura® Device Services, as a file server. In the IP Office environment, the IP Office system can act as a file server for most phones. However, you must use an external HTTP or HTTPS file server for hosting and downloading software distribution packages for Avaya Vantage™ due to the size and number of files.
- Avaya Session Border Controller for Enterprise. This is an optional component.

  Tip:

  You must ensure that Avaya Session Border Controller for Enterprise is configured to accept the new SIP user agent for Avaya Vantage™ Connect. For more information, see Avaya Session Border Controller for Enterprise configuration on page 28.
- A conferencing server, such as Avaya Equinox® Conferencing, for audio and video conference.

Hardware requirements

Ensure that the LAN:

- Uses Ethernet Category 5e or Ethernet Category 6 cabling.
- Has the 802.3at or 802.3af PoE specification.

If your network does not support the 802.3at or 802.3af PoE specification, you can use an AC power adapter, which you can order separately.

Related links

Avaya Aura configuration for Avaya Vantage on page 23
IP Office configuration for Avaya Vantage on page 25
Deployment comparison between Avaya Aura and IP Office on page 26
Avaya Session Border Controller for Enterprise configuration on page 28

Avaya Aura® configuration for Avaya Vantage™

When Avaya Vantage™ is deployed in an Avaya Aura® environment, you can configure the following servers:

- Avaya Aura® System Manager: To create users for Avaya telephony applications, such as Avaya IX™ Workplace Client and Avaya Vantage™ Connect and to use Personal Profile Management (PPM).
- Avaya Aura® Device Services: To use Unified Login to log in to Avaya Vantage™ and to manage contacts.

This does not apply if your deployment uses IP Office.

Avaya Aura® System Manager configuration

Configure the Avaya Aura® System Manager server to:

- Create users for Avaya™ Client SDK telephony applications installed on Avaya Vantage™. You can set up Avaya IX™ Workplace Client or Avaya Vantage™ Connect as the active Avaya™ Client SDK application on your Avaya Vantage™ device.
- Manage public contacts and shared addresses.
- Use Personal Profile Management (PPM).

User configuration to support Avaya IX™ Workplace Client and Avaya Vantage™ Connect as the SIP telephony application

While creating and configuring SIP users in System Manager for the Avaya™ Client SDK application installed on Avaya Vantage™, in the Communication Profile tab, under the CM Endpoint Profile section, use a template with **Set Type** as 9641SIP.

For information about other required fields to configure a user profile, see System Manager user profile worksheet on page 31.

For information about Avaya Aura® System Manager installation and administration, see:

- *Deploying Avaya Aura® System Manager on System Platform*
- *Administering Avaya Aura® System Manager*

PPM configuration

Personal Profile Management (PPM) is a service provided by Avaya Aura® System Manager. PPM is not supported if you do not use Avaya Aura® environment.

Avaya Vantage™ uses PPM to:

- Obtain emergency numbers.
- Obtain configuration parameters that impact the Avaya Vantage™ platform.
- Back up and restore specific user configuration settings, such as language or time format settings. When the user logs in to any registered device, PPM restores user data on the device.

Avaya™ Client SDK applications, such as Avaya Vantage™ Connect, use PPM for the following purposes:

- For contact management, such as retrieving and updating of PPM or Avaya Aura® contacts.
- To obtain emergency numbers and Differentiated Service Code Point (DSCP) values.
- To obtain application configuration parameters.

The PPM server must be reachable for the SIP registration to be successful. Until SIP registration succeeds, Avaya Vantage™ uses IP addresses specified in SIP_CONTROLLER_LIST for the getInitialEndpointConfiguration request. If the PPM server is unreachable, Avaya Vantage™ tries the next IP address from SIP_CONTROLLER_LIST. Similarly, after SIP registration is complete, Avaya Vantage™ uses IP addresses from SIP_CONTROLLER_LIST to perform all other PPM requests.

PPM is disabled if the value of ACTIVE_CSDK_BASED_PHONE_APP is “” (null string), or if the application specified in ACTIVE_CSDK_BASED_PHONE_APP is not installed.

Avaya Aura® Device Services configuration

Configure the Avaya Aura® Device Services server to:

- Use Unified Login credentials for logging in to Avaya Vantage™.
- Manage contacts.

You can use Avaya Aura® Device Services to configure Avaya Vantage™ device and Avaya™ Client SDK application parameters. Parameter configuration through Avaya Aura® Device Services takes priority over the `46xxsettings.txt` file. When using Avaya Aura® Device Services for device configuration, use absolute URLs for configuration parameters that specify file paths for downloads. For example, the TRUSTCERTS parameter value configured in Avaya Aura® Device Services must have the absolute URL format.

You can also use the Utility Server, which is embedded in Avaya Aura® Device Services, as a file server. For information about migrating from Avaya Aura® Utility Services to the new Utility Server, see “Migrating Utility Server data” in *Administering Avaya Aura® Device Services*.

For information about Avaya Aura® Device Services installation and administration, see:

- *Deploying Avaya Aura® Device Services*
- *Administering Avaya Aura® Device Services*

Configurations to support video calls on Avaya Vantage™

To enable video calls on Avaya Vantage™, you must set ENABLE_VIDEO to 1 in the `46xxsettings.txt` file. In the Avaya Aura® environment, additional Communication Manager and System Manager configurations are required to support video calls on Avaya Vantage™.

Signaling group configuration

While configuring Communication Manager signaling groups to be used for communication with Session Manager, you must set **IP Video** and **Initial IP-IP Direct Media** to `y`.

IP codec sets configuration

While configuring Communication Manager IP codec sets to be used by Avaya Vantage™, you must set **Allow Direct-IP Multimedia** to `y`, and **Maximum Call Rate for Direct-IP Multimedia** and **Maximum Call Rate for Priority Direct-IP Multimedia** to `4096` Kbits.

Routing location configuration

While configuring Session Manager home location for a user in System Manager (**Elements** > **Routing** > **Locations**), you must ensure that **Maximum Multimedia Bandwidth (Intra-Location)** and **Maximum Multimedia Bandwidth (Inter-Location)** are set to 4096 Kbits/Sec.

SIP user configuration

While creating and configuring SIP users in System Manager (**Users** > **User Management** > **Manage Users**), in the Communication Profile tab, under the CM Endpoint Profile section, you must select the **Template** as 9641SIP_DEFAULT with the **Set Type** value as 9641SIP.

User extension configuration

In System Manager, you must also enable the IP Video feature for the SIP user's extension.

From **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints**, you can search and modify the configuration for the extension. In the Feature Options tab, enable **IP Video**.

IP Office configuration for Avaya Vantage™

To deploy Avaya Vantage™ in an IP Office environment, the following requirements apply:

- IP Office Server Edition, IP Office Select, or IP500 V2 system running IP Office Release 11.0 or later.

  For Avaya IX™ Workplace Client support on Avaya Vantage™ K165 and K175, you require IP Office Release 11.0.4 or later.

- A separate HTTP or HTTPS file server to host the Avaya Vantage™ firmware and APKs.

  In an IP Office cloud deployment, you can use Google bucket to host firmware and APKs.

For more information, see the following documents:

- *Avaya IP Office™ Platform Solution Description* and *Avaya IP Office™ Platform Feature Description* for general information about IP Office.
- *Avaya IP Office™ Platform SIP Telephone Installation Notes* for information about configuring the IP Office system for Avaya Vantage™.
- *Administering Avaya IP Office™ Platform with Manager* and *Administering Avaya IP Office™ Platform with Web Manager* for information about administering IP Office using IP Office Manager or IP Office Web Manager.

This information does not apply to Avaya Aura® deployments.

Deployment comparison between Avaya Aura® and IP Office

Deployment option or feature	Options with Avaya Aura®	Options with IP Office
File server functionality	You can use: • An external HTTP or HTTPS file server. • Utility Server, which is embedded in Avaya Aura® Device Services, as a file server. For information about: - The Utility Server web interface, see “Working with the Utility Server” in *Administering Avaya Aura® Device Services*. - Migrating from Avaya Aura® Utility Services to the Utility Server in Avaya Aura® Device Services, see “Migrating Utility Server data” in *Administering Avaya Aura® Device Services*.	You can use: • An external HTTP or HTTPS file server. • The IP Office system as the file server for the settings files and an external HTTP or HTTPS file server to host the Avaya Vantage™ software distribution packages. An external HTTP or HTTPS file server is required because the size of the Avaya Vantage™ software distribution packages exceeds the maximum file capacity of IP Office. In the IP Office cloud environment, Google bucket is also supported for hosting firmware packages.

Table continues…

Deployment option or feature	Options with Avaya Aura®	Options with IP Office
Settings file for device configuration	You can manually define configuration parameters in the `46xxsettings.txt` file. Automatic configuration is also available through Avaya Aura® Device Services.	When using IP Office as a file server along with an external HTTP or HTTPs server, you can use the automatically generated `46xxsettings.txt`. Avaya recommends that you do not modify the automatically generated settings file. To define additional configuration parameters or to override the configuration settings from the automatically generated settings file, you can use the `46xxspecials.txt` file. If the `46xxspecials.txt` file is added to the IP Office system SD card, IP Office then automatically adds the `GET 46xxspecials.txt` line at the end of the `46xxsettings.txt` file. The query directs the device to read the settings in the `46xxspecials.txt` file. Alternatively, you can enable querying of the `46xxspecials.txt` file using the NoUser Source Number (NUSN) `ENABLE_46XXSPECIALS_TXT`.
Avaya™ Client SDK telephony applications [1]	Both Avaya Vantage™ Connect and Avaya IX™ Workplace Client are supported.	Both Avaya Vantage™ Connect and Avaya IX™ Workplace Client are supported. For Avaya IX™ Workplace Client support, you need IP Office Release 11.0.4 or later. Only K165 and K175 devices support Avaya IX™ Workplace Client in the IP Office environment.

Table continues…

[1] A feature matrix for Avaya Vantage™ Connect is available in *Using Avaya Vantage™ Connect*.

Deployment option or feature	Options with Avaya Aura®	Options with IP Office
Contact management	You can use Personal Profile Management (PPM) or Avaya Aura® Device Services for managing contacts. Avaya Vantage™ Connect and Avaya IX™ Workplace Client support search for enterprise contacts when contacts are managed through Avaya Aura® Device Services and PPM.	You can manage enterprise contacts as IP Office system contacts and hunt group contacts across a small community network. You can also manage external contacts in LDAP and HTTP directories configured on IP Office. You must define the IPO_CONTACTS_ENABLED parameter to 1 to enable IP Office contacts retrieval by the Avaya™ Client SDK application. Avaya™ Client SDK telephony applications support contact search through the centralized IP Office system directory for enterprise contacts, and the personal directory for the user's personal contact.

For more information about deploying Avaya Vantage™ in the IP Office environment, see *Avaya IP Office™ Platform SIP Telephone Installation Notes*.

Avaya Session Border Controller for Enterprise configuration

The Avaya Session Border Controller for Enterprise (Avaya SBCE) is a network device that controls real-time session traffic between networks. Avaya SBCE manages the endpoints or user agents that are authorized to use a network. If you plan to use Avaya Vantage™ Connect in networks controlled by Avaya SBCE, you must configure the Avaya Vantage™ Connect SIP user agent on Avaya SBCE.

An Avaya Vantage™ Connect SIP user agent uses the `Avaya Vantage Connect/<Application Version> (<Build number>;ro.avaya.product.model;<CSDK version>)` format, where:

- `<Application Version>` is the version of the Avaya Vantage™ Connect application.
- `<Build number>` is the build number of the Avaya Vantage™ Connect application. For example: `0302`
- `ro.avaya.product.model` is the MODEL4 value.
- `<CSDK version>` is the Avaya™ Client SDK version.

The following is an example of the configured Avaya Vantage™ Connect SIP user agent: `Avaya Vantage Connect/2.0.1.0 (0302;K175D02A;261.0.20)`.

In an existing deployment, if you are upgrading the firmware from release 2.0.0.1 or earlier to release 2.0.1 or later with Avaya Vantage™ Connect, you might need to modify the existing user agent rules to authorize the use of Avaya Vantage™ Connect. If an existing rule is defined in a

generic manner that can authorize the Avaya Vantage™ Connect user agent, for example a partial string match to `Avaya Vantage`, then you need not modify the rule.

For more information about configuring user agents on Avaya SBCE, see *Administering Avaya Session Border Controller for Enterprise*.

In the IP Office environment, with Avaya SBCE resiliency, remote workers are not supported if networks are controlled by Avaya SBCE and the SIP controller is defined in an IP address format instead of an FQDN format.

Avaya Vantage™ deployment through Device Enrollment Services

Device Enrollment Services provides a mechanism for Avaya endpoints to be securely authenticated and redirected to a preconfigured provisioning server. The DNS address of Device Enrollment Services is hard-coded to the device firmware. After you connect the out-of-the-box device to the network, Device Enrollment Services redirects the device to the provisioning server and then the installation procedure begins automatically.

For a fresh Avaya Vantage™ device, the trusted certificate repository that is used for configuration and software file downloads using HTTPS is initially empty. With other methods of obtaining the file server address, such as DHCP, LLDP, and manual configuration using the **Settings** menu or the installation wizard, no initial validation of the HTTPS file server certificate occurs until trusted certificates are downloaded to the device. Therefore, Device Enrollment Services is the recommended method for new device deployments for remote users. If you do not use Device Enrollment Services, you must consider staging to download trusted certificates to the fresh device before sending the device to the end user.

For the Device Enrollment Services environment to work, the service provider or enterprise administrator must configure a provisioning server in Device Enrollment Services for the device's MAC address. Alternatively, you can use an enrollment code. For more information about Device Enrollment Services, see *Using Avaya Device Enrollment Services to Manage Endpoints*.

Avaya Vantage™ firmware in Device Enrollment Services

Using Device Enrollment Services, you can ensure that you are using the correct Avaya Vantage™ firmware version. In the Device Enrollment Services web interface, navigate to **Device Family** to view the latest supported firmware version and the minimum version required for device enrollment. For information about enabling automatic firmware upgrades, see "Enabling or disabling device firmware upgrades" in *Using Avaya Device Enrollment Services to Manage Endpoints*.

Configuration for Device Enrollment Services discovery

To enable device discovery, you can configure the DES_STAT parameter in the DHCP Site-Specific Option Number (SSON), which is 242 by default. For a fresh Avaya Vantage™ device to attempt Device Enrollment Services discovery, you can set DES_STAT to one of the following values:

- 2: This is the default parameter value. Device Enrollment Services discovery is triggered when FILE_SERVER_URL, HTTPSRVR, and TLSSRVR are not provided by DHCP or LLDP, and the file server address is not configured through the **Settings** menu.
- 3: Device Enrollment Services discovery is triggered even if FILE_SERVER_URL, HTTPSRVR, or TLSSRVR is retrieved from DHCP or LLDP.

The device attempts to communicate with Device Enrollment Services during startup to obtain the provisioning server address. If the device was not associated with a customer site and activated in Device Enrollment Services, then Avaya Vantage™ prompts for an enrollment code when it is started for the first time. Device Enrollment Services supports an 8-digit or 12-digit enrollment code. The 8-digit code is the most secure. The numbers in this code are randomly generated and it has an expiry date. The 12–digit enrollment code consists of the account ID and a 4-digit PIN. The 12-digit code is easy to remember and does not expire.

After the device startup precess is completed successfully through Device Enrollment Services, the Avaya Vantage™ device communicates with Device Enrollment Services on subsequent reboots to report the device IP address. However, the device does not attempt to obtain the provisioning server address again from Device Enrollment Services unless you perform one of the following:

- Reset the device to its factory defaults.
- Activate the service from **Settings** > **Network & Internet** > **More** > **Auto Provisioning**.

You can disable the Device Enrollment Services discovery for Avaya Vantage™ by setting DES_STAT to one of the following values:

- 0: To disable Device Enrollment Services discovery permanently until you perform a factory reset of the device to the default settings.
- 1: To disable Device Enrollment Services discovery until you activate the service from the device **Settings** menu or set the parameter value to 2 or 3.

Identity certificate generation in Device Enrollment Services

A Public Key Infrastructure (PKI) identify certificate is used to establish a secure connection between the device and the provisioning server. The certificate is required when the provisioning server uses a secure HTTPS connection with mutual authentication. The device receives the certificate from Device Enrollment Services.

When you enable Avaya certificate generation, the device gets the identity certificate from the Avaya Devices Root Certification Authority (CA). If the identity certificate is generated by the

Avaya CA, you can configure a secure connection between the device and the provisioning server. Once the identity certificate is generated, the device will use the new identity certificate. The link to the Avaya CA is https://des.avaya.com/downloads/DeviceEnrollmentServiceRootCA.pem.

The certificate generated through Device Enrollment Services is *only* used for the communication with the provisioning server. It is not used for communication with the customer SIP server or other customer servers.

Preinstallation data

System Manager user profile worksheet

To create a user profile on System Manager for Avaya Vantage™ Connect or Avaya IX™ Workplace Client in the Avaya Aura® environment, you must have the following information:

Identity tab

- **First Name**
- **Last Name**
- **Login Name**
- **Password**
- **Localized Display Name**
- **Endpoint Display Name**
- **Language Preference**
- **Time Zone**

Communication Profile tab

Section	Field
Communication Profile section	**Communication Profile Password**
Communication Address section	**Handle Types** are for: • **Avaya SIP** • **Avaya E.164** • **Avaya Presence/IM** if Presence is used
	Handle Fully Qualified Address
Session Manager Profile section	**Primary Session Manager**
	Secondary Session Manager
	Origination Application Sequence

Table continues…

Section	Field
	Termination Application Sequence
	Survivability Server
	Home Location
CM Endpoint Profile section	**System**
	Profile Type
	Extension
	Use Existing Endpoints
	Template[2]
	Voice Mail Number
Messaging Profile section	**System**
	Mailbox Number
	Template
	Password
	Delete Subscriber on Unassign of Subscriber from User or on Delete User

To support video calls, you must also ensure that video is enabled in the System Manager endpoint configuration.

IP Office SIP user and extension settings

Use IP Office Manager or IP Office Web Manager to configure a SIP user and then configure the extension settings for the user. For information about the key settings to be configured, see *Avaya IP Office™ Platform SIP Telephone Installation Notes* for Release 11.0.

DHCP settings worksheet

You need the following information for dynamically assigning IP addresses to Avaya Vantage™ devices and for the initial configuration that is performed through DHCP options. In the following table, populate the values for your deployment:

Option or parameter	Your value	Notes
Range of IP addresses		
DHCP options		

Table continues…

[2] Use a template with **Set Type** as 9641SIP.

Option or parameter	Your value	Notes
FILE_SERVER_URL		If the HTTP file server requires authentication, you can configure the HTTP credentials with the file server URL through DHCP option 242. Example URL with credentials: http://username:password@example.com/dir_path/
HTTPSRVR		If the FILE_SERVER_URL parameter is defined, Avaya Vantage™ ignores HTTPSRVR and TLSSRVR.
TLSSRVR		If the FILE_SERVER_URL parameter is defined, Avaya Vantage™ ignores HTTPSRVR and TLSSRVR.
DES_STAT		If you want to install the device in a Device Enrollment Services environment and the parameters FILE_SERVER_URL, HTTPSRVR, or TLSSRVR are already defined in the network for use by other endpoints, set DES_STAT to 3.

Settings file worksheet

In the following tables, populate the parameter values suitable for your deployment. These system-wide parameters that you must configure in the `46xxsettings.txt` file are generally required for each Avaya Vantage™ device.

Note:

In the IP Office environment with IP Office as the file server, most of the following parameters are generated automatically. However, TIMEZONE and ACTIVE_CSDK_BASED_PHONE_APP are not part of the automatically generated `46xxsettings.txt` file. ACTIVE_CSDK_BASED_PHONE_APP is part of the automatically generated upgrade file. You can configure additional parameters and override parameters in the automatically generated configuration files using the `46xxspecials.txt` file.

For detailed description of the parameters, see Appendix A, “Supported configuration parameters”.

For some parameter configuration examples, see Appendix B, “Parameter configuration examples in the settings file”.

System settings

Parameter	Your value
FILE_SERVER_URL	
TRUSTCERTS	

Table continues…

Parameter	Your value
ADMIN_PASSWORD or PROCPSWD	
ISO_SYSTEM_LANGUAGE	
ADMINTIMEFORMAT	
TIMEZONE	
COUNTRY	
PUSH_APPLICATION	
ACTIVE_CSDK_BASED_PHONE_APP	Configure this parameter only for environments with Avaya Vantage™ Connect or Avaya IX™ Workplace Client as the active SIP telephony application. If you are using a third-party telephony application, use the default value.
USER_INSTALL_APPS_GOOGLE_PLAY_STORE	

Do *not* set the PUSH_APPLICATION and ACTIVE_CSDK_BASED_PHONE_APP parameters through Avaya Aura® Device Services.

Note:

In the Avaya Aura® environment, if the complex administrator password is configured in System Manager for the specific device deployment location, then Avaya Vantage™ uses the complex password as the administrator password instead of the value defined in ADMIN_PASSWORD or PROCPSWD. If the complex password is not configured in System Manager, Avaya Vantage™ uses ADMIN_PASSWORD or PROCPSWD.

Network settings

Parameter	Your value
DNSSRVR	
DOMAIN	
SNTPSRVR	

Important:

You must configure SNTPSRVR if the default Avaya and NIST SNTP servers are not accessible over the internet. Specifying an SNTPSRVR value that is reachable from your network is essential for SIP registration and initial device setup when you start up Avaya Vantage™.

SIP interface settings

Parameter	Your value	Notes
SIPDOMAIN		
SIP_CONTROLLER_LIST		
SIMULTANEOUS_REGISTRATIONS		For the IP Office environment, set this parameter to 1.

Table continues…

Parameter	Your value	Notes
ENABLE_SIP_USER_ID	0 or 1	Optional. Set this parameter to 1 if you need to distinguish between the SIP user name and SIP user ID for SIP authentication and SIP registration respectively. If you set the parameter to 0, Avaya Vantage™ considers the user name to be identical to the user ID. When you set ENABLE_SIP_USER_ID to 1, the Avaya Vantage™ Login screen displays the following fields: • **Username** for entering the SIP user name. • **Password** for entering the SIP user password. • **Authentication username** for entering the SIP user ID. When you set ENABLE_SIP_USER_ID to 0, the **Authentication username** field is not available to the device user during login.

Server environment settings

Parameter	Your value	Notes
ENABLE_AVAYA_ENVIRONMENT		For the IP Office and Open SIP environments, set this parameter to 0. For the Avaya Aura® environment, accept the default value, 1.
ENABLE_IPOFFICE		For the IP Office environment, set this parameter to 1. For the Avaya Aura® and Open SIP environments, accept the default value, 0.
DISCOVER_AVAYA_ENVIRONMENT		For the IP Office and Open SIP environments, set this parameter to 0. For the Avaya Aura® environment, accept the default value, 1.

Related links

Device configuration using a 46xxsettings.txt settings file on page 111

DHCP server setup

Set up a DHCP server to:

- Dynamically assign IP addresses to Avaya Vantage™ devices.
- Provision device and site-specific configuration parameters through various DHCP options.

In a Device Enrollment Services environment, the DHCP server is mainly used to assign IP addresses to the devices. The device receives the file server address from Device Enrollment Services.

Setting up a DHCP server

About this task

Use this procedure to set up a third-party DHCP server. Avaya Vantage™ supports any DHCP server software as long as the software is correctly configured.

In the IP Office environment, you can use either the IP Office system as the DHCP server or a third-party DHCP server. For more information, see *Avaya IP Office™ Platform SIP Telephone Installation Notes*.

Before you begin

Get the following from your server software vendor:

- All required licenses for the server software.
- Instructions for server software installation and configuration.

Procedure

1. Install the DHCP server software according to the server software vendor's instructions.
2. Create a DHCP scope to define the range of IP addresses to use.

   You can define different scopes from different types of devices.
3. Configure the required DHCP options.

   The DHCP site-specific option that you configure must match the Site Specific Option Number (SSON) that Avaya Vantage™ uses. The default SSON that Avaya Vantage™ uses is 242.

File server setup

A file server is an HTTP or HTTPS server that is used for downloading and storing software distribution packages, `K1xxSupgrade.txt` and `46xxsettings.txt` files that contain most of the device configuration, and other files required for Avaya Vantage™ devices. When Avaya Vantage™ starts or restarts, it checks for software updates and settings files on the specified file

servers. Therefore the file server address is the most important configuration for the device deployment.

Important:

While setting up a file server for Avaya Vantage™, you must take into consideration the following:

- Memory space available on the file server.
- Size of the extracted software distribution packages, that include the firmware and `.apk` files.

  The size of the software distribution package that is meant for K155, K165, and K175 combined is approximately 1 GB.
- Size of additional application `.apk` files you want to install.
- Size of other media files that you might use, such as ringtones and wallpapers.

File server address configuration

You can provide file server addresses using one of the following methods:

- DHCP
- LLDP
- The **Settings** menu on the Avaya Vantage™ device
- Device Enrollment Services
- `46xxsettings.txt` settings file
- Avaya Aura® Device Services for Avaya Aura®

You can also provide this information using the Android installation wizard on K165 and K175 devices.

In a Device Enrollment Services environment, Device Enrollment Services redirects the device to the file server to be used. The service provider or enterprise administrator configures the file server in Device Enrollment Services for the device. Device Enrollment Services supports a file server URL in either the FQDN or IP address format. While the file server can be an HTTP or HTTPS server, Avaya recommends that you use HTTPS with an FQDN. For more information about Device Enrollment Services, see *Using Avaya Device Enrollment Services to Manage Endpoints*.

The FILE_SERVER_URL parameter is used to assign the file server address. For LLDP, you can specify the file server address in the file server TLV.

You can also specify the file server address using the following parameters:

- HTTPSRVR, HTTPDIR and HTTPPORT parameters for an HTTP server.
- TLSSRVR, TLSDIR and TLSPORT parameters for an HTTPS server.

If the FILE_SERVER_URL parameter is defined, Avaya Vantage™ ignores all other parameters.

If the HTTP file server requires authentication, you can configure the HTTP credentials with the file server URL through DHCP option 242. If you do not configure the HTTP credentials through DHCP, Avaya Vantage™ displays a notification to the user at the device startup to enter the

credentials. In addition, the Android installation wizard provides you option to enter the HTTP credentials for a file server that requires authentication.

Utility Server as the file server

In the Avaya Aura® environment, you can use the Utility Server as a file server. The Utility Server is now embedded in Avaya Aura® Device Services. For information about migrating from the legacy Avaya Aura® Utility Services to the new Utility Server, see “Migrating Utility Server data” in *Administering Avaya Aura® Device Services*.

You must include the root CA certificate of the Utility Server identity certificate in TRUSTCERTS.

The Utility Server web interface does not support upload of zip files larger than 800 MB. If you have problems uploading the Avaya Vantage™ software distribution package file, see Software distribution packages cannot be uploaded using the Utility Server on page 185.

IP Office system as the file server

In the IP Office environment, Avaya Vantage™ can accept settings files, including `K1xxSupgrade.txt` and `46xxsettings.txt`, from the IP Office system as a file server. However, Avaya Vantage™ requires an external HTTP or HTTPS file server for hosting and downloading software distribution packages due to the size and number of files. The address of the IP Office system is used as the file server address for the device. The IP Office system then redirects the request for firmware files to the configured HTTP or HTTPS server IP address on the IP Office system. In this dual server configuration mode, you get the option of using the auto-generated `46xxsettings.txt` file.

For more information about setting up the file server in the IP Office environment, see *Avaya IP Office™ Platform SIP Telephone Installation Notes*.

Setting up a file server

About this task

Use this procedure to configure an HTTP or HTTPS file server. The file server is used to download and store distribution packages and settings files for Avaya Vantage™.

Avaya Vantage™ supports any HTTP or HTTPS server software as long as the software is correctly configured.

Before you begin

Get the following from your server software vendor:

- All required licenses for the server software.
- Instructions for server software installation and configuration.

Procedure

1. Install the HTTP or HTTPS server software according to the server software vendor’s instructions.

   For HTTPS connections, ensure that TRUSTCERTS includes the root CA certificate of the HTTPS file server identity certificate.

After trusted certificates are downloaded, then the HTTPS file server identity certificate is verified. You must use Device Enrollment Services for secure redirection or use staging to download trusted certificates in a secure environment first.

2. Download the software distribution package and the `46xxsettings.txt` settings file.
3. Extract the distribution package and save the extracted files and the `46xxsettings.txt` settings file on the file server.

Downloading device firmware

Before you begin

Ensure that your file server is set up.

Procedure

1. Go to the Avaya Support website.
2. In the **Enter Product Name** field, enter `Avaya Vantage`.
3. In the **Choose Release** field, click the required release number.

   The site displays a list of the latest downloads.

Do the following to download a firmware package:

4. In the Downloads section, click the entry with the required firmware version.

   The site displays the Downloads page with the information about the selected firmware version and the list of package files available for downloading.
5. In the **File** field, click the zipped file and save the file on the file server.
6. Extract the zipped file and save it at an appropriate location on the file server.

Do the following to download the `46xxsettings.txt` file:

7. In the Downloads section, click the entry with the `46xxsettings.txt` file.

   The site displays the Downloads page with information about the settings file software version and the link for downloading the settings file.
8. In the **File** field, click the `46xxsettings.txt` file link, and save the file at an appropriate location on the file server.

Configuring parameters in the settings file

About this task

Use this procedure to modify the settings file with appropriate values to provision the device configuration parameters.

Procedure

1. On the file server, go to the location where the `46xxsettings.txt` file is downloaded.
2. Open the `46xxsettings.txt` file in a text editor.
3. Set the required parameters as the following:

   ```
   SET <parameter_name> <parameter_value>
   ```

   For more information about the supported configuration parameters, see “Appendix A, Supported configuration parameters”.
4. Save the `46xxsettings.txt` file.

Result

On the next polling period, Avaya Vantage™ downloads the file and applies the settings.

Related links

Customization of the settings file on page 112
User group configuration in the settings file on page 114

SNTP server setup

Avaya Vantage™ must have access to an SNTP server for time synchronization. Receiving the correct time is essential for Avaya Vantage™, especially when the device uses SIP-TLS connectivity with the SIP controller. The start time of the SIP controller identity certificate must be earlier than the current device time. Otherwise, the SIP-TLS connection fails.

The SNTPSRVR parameter provides the SNTP server addresses to Avaya Vantage™. You can configure the SNTPSRVR parameter using one of the following options, which are listed in order of precedence, from the lowest to the highest priority:

- DHCP option 42.

  If you are using DHCPv6, a `name=value` pair in DHCPv6 Reply VSI option 242.
- `46xxsettings.txt` file.
- Avaya Aura® Device Services configuration or the **Settings** menu.

  You must be in the administrator mode to configure the SNTP server addresses through the **Settings** menu.

For example, if you set the SNTP server addresses through the **Settings** menu, the device tries to retrieve time from those addresses instead of the addresses you set through the `46xxsettings.txt` file.

The value of the SNTPSRVR parameter can be a comma-separated list of SNTP server addresses, which can be IPv4 or IPv6 addresses, or FQDNs. The parameter has the following default value:

```
"0.avaya.pool.ntp.org,1.avaya.pool.ntp.org,2.avaya.pool.ntp.org,3.avaya.
pool.ntp.org,129.6.15.28,132.163.97.1"
```

If you cannot reach the default SNTP servers, you must update the SNTPSRVR value to point to one or more SNTP servers that are accessible from your network.

If no SNTP server is available on your network, you can set up your own SNTP servers. Configure your SNTP servers according to the vendor's configuration instructions. You must ensure that the SNTP server is reachable from the network where you are installing Avaya Vantage™.

Avaya Vantage™ can also try to retrieve time from HTTP or HTTPS based services that the device accesses *before* the SIP-TLS registration.

The following are the time retrieval sources for Avaya Vantage™ in order of precedence:

- SNTP servers that you configured through SNTPSRVR.
- Default SNTP servers.

  The device tries to retrieve time from these default servers only if you have not configured SNTP server addresses through SNTPSRVR or the configured SNTP servers are not reachable.
- HTTP or HTTPS based services that the device accesses.

  If the default or configured SNTP servers are also not accessible, the device uses the *first* valid time in the HTTP Date header received from an HTTP or HTTPS service. The device considers the time from an HTTP or HTTPS server as valid if it has a newer time than the embedded device time. The following are the HTTP or HTTPS servers that the device accesses in order:

  - Device Enrollment Services.
  - HTTP or HTTPS file server for configuration and software file download.
  - Avaya Aura® Device Services when USER_AUTH_FILE_SERVER_URL is configured.
  - PPM.

The Date & Time Status section on the Configuration verifier screen indicates whether time retrieval from the configured SNTP server is successful. If the Avaya Vantage™ device receives time from a source other than the configured SNTP servers, such as a default SNTP server or an HTTP-based service, the Configuration verifier screen indicates that.

IP address configuration

In an Avaya Aura® deployment, Avaya Vantage™ and the active Avaya™ Client SDK application on Avaya Vantage™ can now work and internetwork in IPv4 and IPv6 mode. Avaya Vantage™ supports the following combinations of IPv4 and IPv6 IP address configuration:

- IPv4 only mode.
- IPv6 only mode.

- Dual-stack mode: Both IPv4 and IPv6 addresses are supported.

In an IP Office deployment, Avaya Vantage™ does not support IPv6.

Note:

Avaya Vantage™ supports IPv6 on the Ethernet interface only. It does not support IPv6 on Wi-Fi interfaces.

IPv6 address auto-configuration

The IPv6 address auto-configuration process for the Avaya Vantage™ device includes generating a link-local address, global addresses using stateless address auto-configuration (SLAAC), and the Duplicate Address Detection (DAD) procedure for verifying that the addresses are unique.

On the Avaya Vantage™ device, you can configure IPv6 address assignment to the interface in the following ways:

- Using DHCPv6 or static addressing
- Using SLAAC

You can use both DHCPv6 and SLAAC simultaneously. The device can have multiple IPv6 addresses, all of which can be SLAAC.

Through the device **Settings** menu, you can manually enable the following:

- DHCP or static addressing for IPv4 address configuration.
- DHCPv6 or static addressing for IPv6 address configuration.
- SLAAC for automatic IPv6 address configuration.

Parameter configuration to support IPv6 operation

Set the following parameters to define IPv6 operation support for Avaya Vantage™ and the active Avaya™ Client SDK application on the device:

Parameter	Default value	Description
IPV6STAT	1	Specifies the mode of the IP family to be used in the current device configuration. Assign on of the following values: • 0: Support IPv4 only mode. • 1: Support dual mode (IPv4 and IPv6). • 2: Support IPv6 only mode. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

Table continues…

Parameter	Default value	Description
DHCPSTDV6	0	Specifies whether DHCPv6 will comply with the IETF RFC 8415 standard and immediately stop using an IPv6 address if the address valid lifetime expires, or whether it will enter an extended rebinding state. Assign on of the following values: • 0: If the DHCPv6 lease expires, DHCPv6 enters a proprietary extended rebinding state, in which it continues to use the IPv6 address. • 1: If the DHCPv6 lease expires, DHCPv6 complies with the IETF RFC 8415 standard and immediately releases the IPv6 address. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.
DHCPSTAT	3	Specifies whether DHCPv4, DHCPv6, or both are to be used to assign IP addresses to the device. Assign on of the following values: • 1: Run only DHCPv4. • 2: Run only DHCPv6. • 3: Run both DHCPv4 and DHCPv6. In IPv4 only mode, if you set DHCPSTAT to 2, DHCPv4 is disabled. You cannot enable the use of DHCP through the device's **Settings** menu. Only the option for static IPv4 address configuration becomes available. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

Table continues…

Parameter	Default value	Description
PRIVACY_SLAAC_MODE	1	Specifies the preference for privacy extensions (RFC3041) when using SLAAC to generate IPv6 addresses. Assign on of the following values: • 0: Disable privacy extensions. One stable address is generated using modified EUI-64 format interface identifier based on the device MAC address. The device address selection preference is based on default RFC6724 SASA rules. • 1: Enable privacy extensions with a preference for public addresses over temporary addresses. One stable address is generated using modified EUI-64 format interface identifier based on the device MAC address and one temporary private address is generated. This parameter value overrides the default RFC6724 SASA Rule 7 to prefer a manual, DHCPv6, or stable SLAAC address over a SLAAC temporary address. • 2: Enable privacy extensions with a preference for temporary addresses over public addresses. One stable address is generated using modified EUI-64 format interface identifier based on the device MAC address and one temporary private address is generated. The device address selection preference is based on default RFC6724 SASA rules. The default SASA rule 7 is used to prefer a SLAAC temporary address over manual, DHCPv6, or stable SLAAC addresses. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.
DUAL_IPPREF	4	Specifies IPv4 or IPv6 preferences. The parameter controls the selection of SSON either from DHCPv4 or DHCPv6 when the device is in dual mode. DHCP clients use DUAL_IPPREF to decide which SSON configuration attributes to apply for DHCPv4 and DHCPv6 interworking in dual mode. Assign on of the following values: • 4: Prefer IPv4 over IPv6. • 6: Prefer IPv6 over IPv4. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

Table continues…

Parameter	Default value	Description
SIGNALING_ADDR_MODE	4	Specifies IPv4 or IPv6 preference for SIP registration. This parameter comes into effect only when both the device and Session Manager are in dual mode with both IPv4 and IPv6 addresses configured. Based on the value of the parameter, the Avaya™ Client SDK application uses the preferred IP addresses of Session Manager from SIP_CONTROLLER_LIST. Assign on of the following values: • 4: Prefer IPv4 over IPv6. • 6: Prefer IPv6 over IPv4. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. If Avaya Vantage™ is in IPv4 or IPv6 only mode, it ignores SIGNALING_ADDR_MODE. If Avaya Vantage™ is in IPv4 only mode, and Session Manager is either in IPv4 only or dual mode, then the SIP controller's IPv4 addresses are selected from SIP_CONTROLLER_LIST for SIP registration. If Session Manager is in IPv6 only mode, the Avaya™ Client SDK application cannot connect with the SIP controller. If Avaya Vantage™ is in IPv6 only mode, and Session Manager is either in IPv6 only or dual mode, then the SIP controller's IPv6 addresses are selected from SIP_CONTROLLER_LIST for SIP registration. **Important:** To avoid multiple registrations to the same SIP controller over IPv4 and IPv6 addresses, you must configure *only* IPv4, IPv6, or FQDN addresses for each SIP controller in SIP_CONTROLLER_LIST through all provisioning sources. Do not configure mix of IPv4 and IPv6 addresses for the same SIP controller. For provisioning, use: • The value stored on the PPM server. • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. • A `name=value` pair in a DHCPACK message. • DHCPv6 Reply VSI option 242.

Table continues…

Parameter	Default value	Description
MEDIA_ADDR_MODE	4	Specifies the preference of SDP media group lines by the active Avaya™ Client SDK application on Avaya Vantage™. If Avaya Vantage™ is in IPv4 or IPv6 only mode, it ignores MEDIA_ADDR_MODE. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. Assign on of the following values: • 4: Use IPv4. • 6: Use IPv6. • 46: Prefer IPv4 over IPv6. • 64: Prefer IPv6 over IPv4. For provisioning, use: • The value stored on the PPM server. • The **`SET`** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. • A `name=value` pair in a DHCPACK message. • DHCPv6 Reply VSI option 242.
IPV6DADXMITS	1	Specifies whether Duplicate Address Detection (DAD) is performed on tentative addresses, as specified in RFC 4862. A non-zero value specifies the maximum number of transmitted Neighbor Solicitation (NS) messages to determine whether an IPv6 address is already in use. The value can be in the range from 0 to 5. Assign on of the following values: • 0: Disable DAD. • 1 to 5: Enable DAD. The value indicates the maximum number of transmitted NS messages. For provisioning, use: • The **`SET`** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

Configuring IPv4 through the Settings menu

About this task

You can use DHCP or static IPv4 addressing to assign IPv4 address to the device's IP interface. When you disable DHCP, you must manually enter the device IPv4 address, subnet mask, and IPv4 gateway.

Procedure

1. From the **Settings** menu, navigate to **Network & Internet** > **Ethernet**.
2. Tap **IP interface**.
3. **(Optional)** Enable administrator mode.

   If some of the fields are locked or obscured, you must use the administrator password to access these fields.
4. Do one of the following to configure the IPv4 address:
   - To use DHCP, enable **Use DHCP**.
   - To use static IPv4 addressing, disable **Use DHCP**, tap **Static IP settings**, and complete the following fields:
     - **IPv4 Address**
     - **Netmask**
     - **Default router**

   The device takes approximately 5 seconds to refresh and retrieve the updated IP configuration.

Configuring IPv6 through the Settings menu

About this task

You can use DCHPv6 or static IPv6 addressing and SLAAC to assign IPv6 addresses to the device's IP interface.

Procedure

1. From the **Settings** menu, navigate to **Network & Internet** > **Ethernet**.
2. Tap **IP interface**.
3. **(Optional)** Enable administrator mode.

   If some of the fields are locked or obscured, you must use the administrator password to access these fields.

4. Do one of the following to configure IPv6 addresses:
   - To use DHCPv6, enable **Use DHCPv6**.
   - To use static IPv6 addressing, disable **Use DHCPv6**, tap **Static IPv6 settings**, and complete the following fields:
     - **IPv6 Global Address**
     - **Prefix Length**
5. To use SLAAC addresses for the device, enable **Use SLAAC**.

   You can enable both DHCPv6 and SLAAC simultaneously. You can also use SLAAC with static IPv6 addressing.

   The device takes approximately 5 seconds to refresh and retrieve the updated IP configuration.

Power and network connectivity

The following sections describe how to power up your Avaya Vantage™ device and connect it to the network.

Power management

Avaya Vantage™ can receive power from the following sources:

- 802.3af PoE (Class 3)
- 802.3at PoE (Class 4)
- 48 Vdc power supply

If you use the 802.3at networking switch or the power adapter, Avaya Vantage™ USB port delivers up to 500mA. If you use the 802.3af networking switch, Avaya Vantage™ USB port delivers up to 100mA.

You can use a 48-volt, 30-watt power adapter to power Avaya Vantage™ in the following conditions:

- You are using Wi-Fi to connect to the network instead of using a PoE networking switch port.
- The networking switch port does not support the 802.3af or 802.3at PoE specification.
- The device requires more power than a 802.3af PoE networking switch port can provide, and 802.3at PoE port is unavailable. For example, a USB device that requires more than 0.5 watts is connected to Avaya Vantage™ and only 802.3af PoE ports are available. In this case, you must connect Avaya Vantage™ to a power adapter.

You must purchase the power adapter separately.

If Avaya Vantage™ is connected to both a 48 Vdc power supply and a PoE networking switch port and you disconnect one of the power sources, then the following occurs:

- If you disconnect the power adapter, Avaya Vantage™ reboots. If the networking switch supports the 802.3at or 802.3af specification, Avaya Vantage™ continues to work after the reboot.
- If you disconnect the networking switch, Avaya Vantage™ continues to work without a reboot.

If Avaya Vantage™ is already connected to a PoE networking switch and you connect the power adapter to the device, Avaya Vantage™ continues to work without a reboot.

Connecting the Avaya Vantage™ device to the network

About this task

Use this procedure to install your Avaya Vantage™ device on your network. The procedure also describes how to go through the Device Enrollment Services discovery process for automatic setup of the device.

Before you begin

Ensure that the required phone hardware is set up.

If you are using Device Enrollment Services and Device Enrollment Services is configured to use a numeric enrollment code, get the numeric enrollment code.

If installing without Device Enrollment Services discovery, ensure the following:

- Required phone hardware is set up.
- File server is configured.
- Firmware package is downloaded and extracted to the file server.
- The settings file is configured for the deployment environment.

Procedure

1. **(Optional)** Connect a power adapter to the 48-V DC power connector at the back of the device and plug the power adapter into an electrical outlet if:
   - Your network does not support the 802.3at (PoE) or 802.3af (PoE) injector specification.
   - You want to use a Wi-Fi connection.
2. To use a wired Ethernet connection, plug one end of an Ethernet cable into the LAN port at the back of Avaya Vantage™ and the other end into an available LAN port on your network.

   Avaya Vantage™ powers up and starts to initialize.
3. **(Optional)** If prompted, enter the Device Enrollment Services enrollment code.

   Device Enrollment Services supports an 8 or 12-digit enrollment code. After you enter the code, Device Enrollment Services provides the file server address. If you do not enter the enrollment code and tap **Cancel** instead, the Device Enrollment Services process is cancelled and you must configure the device manually.

Result

After the device receives the configuration file server address, it starts downloading the required configuration files and updated firmware files from the file server. When there is a software image upgrade, the process can take approximately 1 hour. If there is no software upgrade, the startup process typically takes between 4 to 20 minutes. After the configuration is complete, the device displays a background, which indicates that you can now log in and use the device.

If the device does not receive the file server configuration from Device Enrollment Services, the Android installation wizard is displayed to help you set up your K165 and K175 devices. The wizard is not available on K155 devices.

Installation wizard considerations

When you start a new device for the first time or perform a factory reset, the K165 and K175 devices present an installation wizard to help you set up your device. If the key configuration for the device is already completed, then the installation wizard is not displayed.

If the file server and ACTIVE_CSDK_BASED_PHONE_APP are configured and the Avaya™ Client SDK application is installed, then the installation wizard is not displayed. In this case, you can log in to the device right away using your SIP or enterprise user credentials.

If automatic redirection to the file server through Device Enrollment Services discovery is successful, the installation wizard is not displayed.

If the file server is not configured using DHCP, LLDP, or Device Enrollment Services discovery, then the installation wizard can help you to complete the file server configuration.

Setting up K165 or K175 using the Android installation wizard

About this task

When you power up a new K165 or K175 device for the first time or perform a factory reset, and the device configuration is not complete, the Android installation wizard is displayed to help you set up your K165 or K175 device.

For more information about when the installation wizard is displayed, see Installation wizard considerations on page 50.

Note:

The installation wizard is not currently available on K155 devices. On K155, you can configure the file server manually from **Settings** > **Network & Internet** > **More** > **File Server**.

Procedure

1. On the Welcome screen, choose your preferred language and tap **Start**.
2. If prompted, on the Network Mode Selection screen, choose how you want to connect to the network.

3. **(Optional)** If you set the network mode to Wi-Fi, do the following to connect to a Wi-Fi network:
   a. On the Connect to Wi-Fi screen, select the required network from the available Wi-Fi networks.
   b. For a network that requires authentication, enter the network credentials and select the appropriate CA certificate option from the following:
      - **Use system certificates**
      - **Do not validate**
      - **List of trusted certificates installed on Wi-Fi certificate repository**, if available

        On a new device, no trusted certificates are installed in the repository, so you cannot select this option.
   c. Tap **Connect**.
4. On the Copy apps & data screen, choose one of the following:
   - **Copy your data**: Use this option to restore user-defined device configuration, such as language settings and application data, which is backed up using a personal account, such as a Google account.
   - **Set up as new**: Use this option to set up the device as a new device.
5. Follow the prompts on the wizard screens to set up Google accounts and services.
6. On the Avaya Vantage Configuration screen, verify and update the following configuration information as needed:
   - **File Server**: The configuration file server address. This value is populated when Avaya Vantage™ receives file server information through DHCP or Device Enrollment Services. If you want the device to point to a different file server, modify the **File Server** value.

     You can enter an IP address in the dotted-decimal (IPv4) or colon-hex (IPv6) format, or a Fully Qualified Domain Name (FQDN).

     You can also configure the file server manually from **Settings** > **Network & Internet** > **More** > **File Server**.
   - **Credentials**: User name and password that the device uses for file server authentication. Provide these credentials if the file server requires HTTP authentication.
   - **GROUP**: The user group identifier for a specific configuration set for the device. Enter the required user group identifier from the configuration sets available in the settings file.
   - **File Server Configuration Source**: The source through which the device receives the file server address. This field is ready-only.
7. **(Optional)** Tap **Advanced** to view additional configuration information.

   The device receives file server configuration information through DHCP or Device Enrollment Services. The following values are automatically populated:
   - **DHCP Site Specific Option Number (SSON)**: The DHCP option to set site-specific configuration parameters. In most cases, DHCP option 242 is displayed.

- **DNS Server** and **DNS Domain**: The DNS server address and domain used in your organization.

8. Tap **Next**.

Result

The device starts downloading the required configuration files and updated firmware files from the file server. The device might restart as it loads the updated firmware files. When there is a software image upgrade, the process can take approximately 1 hour. If there is no software upgrade, the startup process typically takes between 4 to 20 minutes. After the configuration is complete, the device displays a background, which indicates that you can now log in and use the device.

Installing the K155 wireless module

About this task

Use this procedure to install the wireless module on the K155 device for Wi-Fi and Bluetooth connectivity. The wireless module is an optional component and you can order this module separately.

This procedure is not applicable for the K165 and K175 devices.

Before you begin

Get a flat screwdriver that fits into the opening of the module panel.

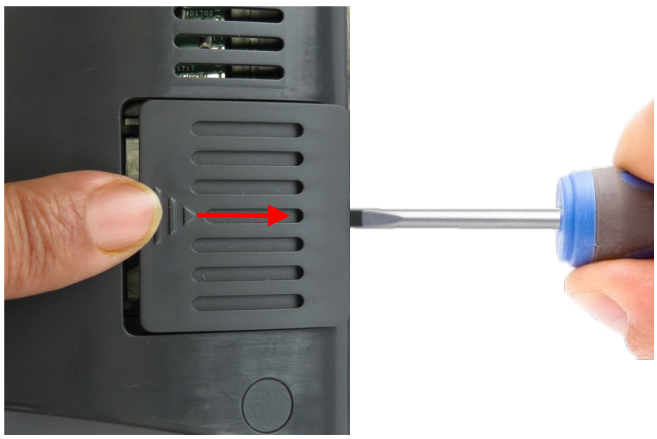
Ensure that the K155 device is not connected to a power source.

Procedure

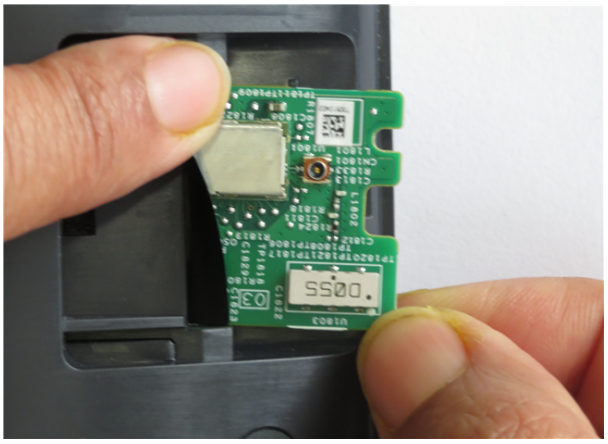
1. Insert the screwdriver into the opening of the module panel to release the latch.

   Do not pry open the panel.

2. To remove the module panel, slide the panel out in the direction of the arrow.



3. Insert the wireless module into the slot.



4. Slide the module panel inward to close it.

   You do not need a screw to fasten the module. The inside of the module panel has a small protrusion that keeps the module in place.

Configuring Wi-Fi from the Settings menu

About this task

Use this procedure to configure a Wi-Fi network using the **Settings** menu on the device.

Procedure

1. Tap **Settings**.
2. Tap **Network & Internet** > **Network mode**.
3. Select **Wi-Fi**.

4. On the Network & Internet screen, tap **Wi-Fi**, and choose the required network.
5. For a network that requires authentication, enter the network credentials and select the appropriate CA certificate option from the following:
   - **Use system certificates**
   - **Do not validate**
   - **List of trusted certificates installed on Wi-Fi certificate repository**, if available

     On a new device, no trusted certificates are installed in the repository, so you cannot select this option.
6. Tap **Connect**.

   If the credentials are authenticated successfully, the device connects to the Wi-Fi network.

Handset connection to Avaya Vantage™

Avaya Vantage™ provides a built-in speaker and microphone, so a handset is not required to make and manage calls. You can purchase either wired or wireless handsets separately. The handsets come with a cradle kit. To use a handset with Avaya Vantage™, you need to connect the handset cradle with the device.

Connecting the handset cradle to Avaya Vantage™

About this task

Use this procedure to connect your handset cradle to the Avaya Vantage™ device. The handset cradle is required for both wired and wireless handsets.

Warning:

When installing the cradle, be careful not to bend the Avaya Vantage™ connector pins.

Before you begin

- Ensure that you have the following equipment:
  - Avaya Vantage™ device.
  - Handset cradle with a connection cable.
  - Handset cradle stand, which varies according to the device variant.

    For K165 or K175, use the adjustable cradle stand with the crossbar that comes with the handset kit. For K155, use the fixed-angle cradle stand that comes with the device.
- Ensure that the Avaya Vantage™ device is not connected to a power source.

Procedure

1. Place the device with the right side touching the table top so that the left side, which is where the handset cradle must be attached, is facing up.
2. On the left side of the Avaya Vantage™ device, remove the rubber gasket that protects the cradle connector pins.

   One cradle connector pin is closed so that you can position the cradle in the correct direction.
3. Connect the handset cradle cable to the cradle connector of the Avaya Vantage™ device.

   Tip:

   Bend the cradle cable to make an arc so that you can join the cable with the cradle connector easily.
4. Connect the cradle to the Avaya Vantage™ device while ensuring that the connection cable is not squeezed between the cradle and the device.
5. **(Optional)** For K165 or K175, connect the handset cradle stand crossbar to the slot in the Avaya Vantage™ stand.
6. Connect the handset cradle to the cradle stand using the hinge on the rear panel of the cradle.

Next steps

Connect Avaya Vantage™ to the power source.

Connecting a wired handset

About this task

Use this procedure to connect a wired handset to your Avaya Vantage™.

Before you begin

Ensure that the handset cradle is connected to the Avaya Vantage™ device.

Procedure

1. Plug the non-spiral end of the handset cord into the handset connector on the handset cradle.
2. Plug the other end into the connector on the handset.

Connecting a wireless handset

About this task

Use this procedure to connect or pair a wireless handset with your Avaya Vantage™ device. After pairing a wireless handset with your Avaya Vantage™ device, you cannot use the wired handset. You can pair only one wireless handset with a device at a time.

After you complete this procedure, you can use your wireless handset for calls as long as the handset is turned on. When the handset is turned off, you cannot use it for calls, but it is still paired with Avaya Vantage™.

Before you begin

- Log in to your Avaya Vantage™ device.
- Connect the handset cradle to your Avaya Vantage™ device.
- Charge the handset battery by placing the handset in the cradle.
- Ensure that the wireless handset is turned off.

Procedure

1. Lift the wireless handset from the cradle, and press and hold the top **Power** button for at least 10 seconds to enter the pairing mode.

   To indicate that the handset is in the pairing mode, the handset LED starts flashing.

2. On the Home screen, tap **Applications**.

3. Tap **Settings** > **Connected devices** > **Bluetooth**.
4. Turn Bluetooth on.
5. In the list of available devices, tap the entry that matches the ID on the handset label.

   When pairing is successful, the list of paired devices indicates that the wireless handset is connected.

Related links

Enabling a wireless handset upgrade on page 183

Removing the pairing with the wireless handset

About this task

Use this procedure to remove the pairing between your Avaya Vantage™ device and the wireless handset. After you remove the pairing, you can connect and use a wired handset with your device or pair the wireless handset with another device.

Before you begin

Ensure the following:

- Bluetooth is enabled on the device.
- The wireless handset is turned on.

Procedure

1. Tap **Settings** > **Connected devices** > **Bluetooth**.
2. In the list of paired devices, tap ⚙ next to the entry for the paired wireless handset.

   The list displays the paired handset entry as `Avaya J100-<ID>`.
3. Tap **FORGET**.

   The device removes the wireless handset from its list of paired devices.

Wall mounting options for Avaya Vantage™

Avaya Vantage™ comes with an adjustable stand that you can use as a desk stand or a wall-mount. You do not need to order a separate wall-mount kit for the device. The stand has two standard wall-mount slots built in. You can mount your device to the wall using:

- Two screws vertically spaced 4 inches apart.
- A standard dual-stud telephone wall plate that is installed on the wall.

To wall mount the device along with a handset cradle, you need a wall-mount bracket for the cradle. You must remove the tilt stand from the cradle and use the wall-mount bracket to affix the cradle to the wall. You can purchase the wall-mount bracket for the cradle separately from Avaya.

Mounting Avaya Vantage™ directly on a wall

About this task

You can wall mount Avaya Vantage™ using two screws or a telephone wall plate. This procedure describes how to wall mount Avaya Vantage™ using screws. The device stand has two standard wall-mount slots where you can fit these screws.

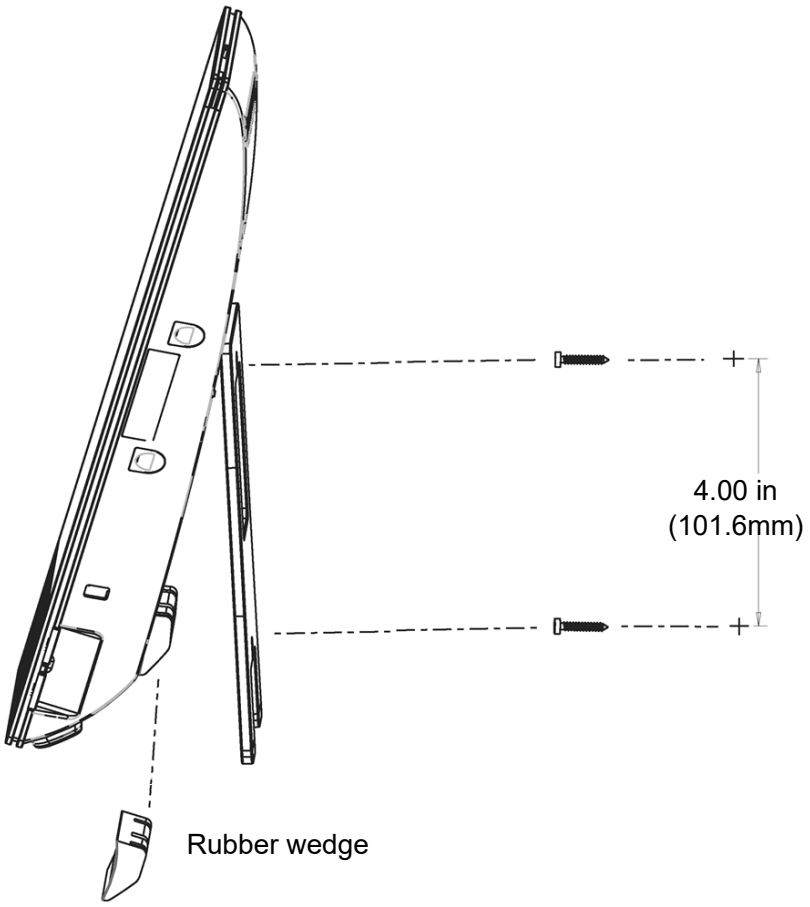
Before you begin

Ensure that you have the following items:

- The two screws included with the device in the box.
- A rubber wedge included with the device in the box.
- Phillips-head screwdriver.
- Pencil.
- An Ethernet cable.

Procedure

1. Use a pencil to mark two screw holes that are vertically spaced at 4 inches apart.



2. Drill holes and use a Phillips-head screwdriver to install the screws in the wall.
3. Attach the rubber wedge to the back of the Avaya Vantage™ device towards the base as shown in the above image.

   The rubber wedge has a self-adhesive area that you can attach to the surface of the device. It stabilizes the wall-mounted device to prevent movement when you touch or tap the screen.
4. Plug the Ethernet cable to the LAN port on the rear panel of the device.
5. **(Optional)** If you are using an external power supply or an RJ9 headset, connect the power adapter cord or the headset to the device.

   These ports are on the rear panel of the device, which are not accessible when the device is wall mounted. Therefore, carry out this step before you mount the device.
6. Close the device stand to make it rest on the rubber wedge.
7. Place any dangling cables through the cable-access openings at the bottom of the stand and around the rubber wedge.
8. Align the wall-mount slots on the device stand with the screws fitted on the wall and slide the device down until it mounts securely on the screws.

Mounting Avaya Vantage™ on a wall plate

About this task

You can wall mount Avaya Vantage™ using two screws or a telephone wall plate. This procedure describes how to mount Avaya Vantage™ on a pre-installed standard dual-stud telephone wall plate.

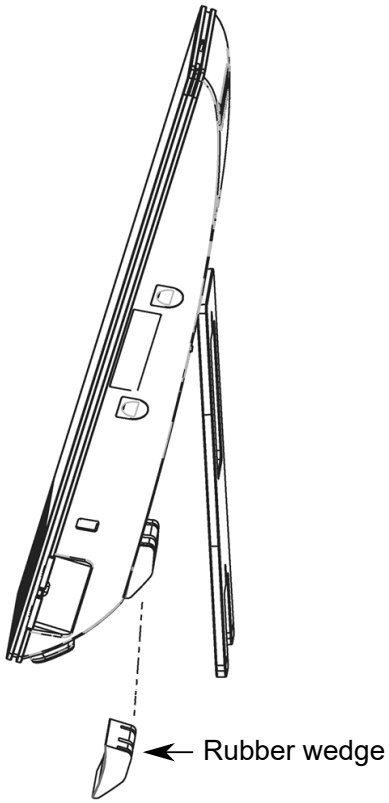
Before you begin

Ensure that you have the following items:

- A rubber wedge included with the device in the box.
- A short Ethernet cable, between 4 to 12 inches long, with short RJ45 connectors.
- A standard dual-stud telephone wall plate that is installed on the wall.

Procedure

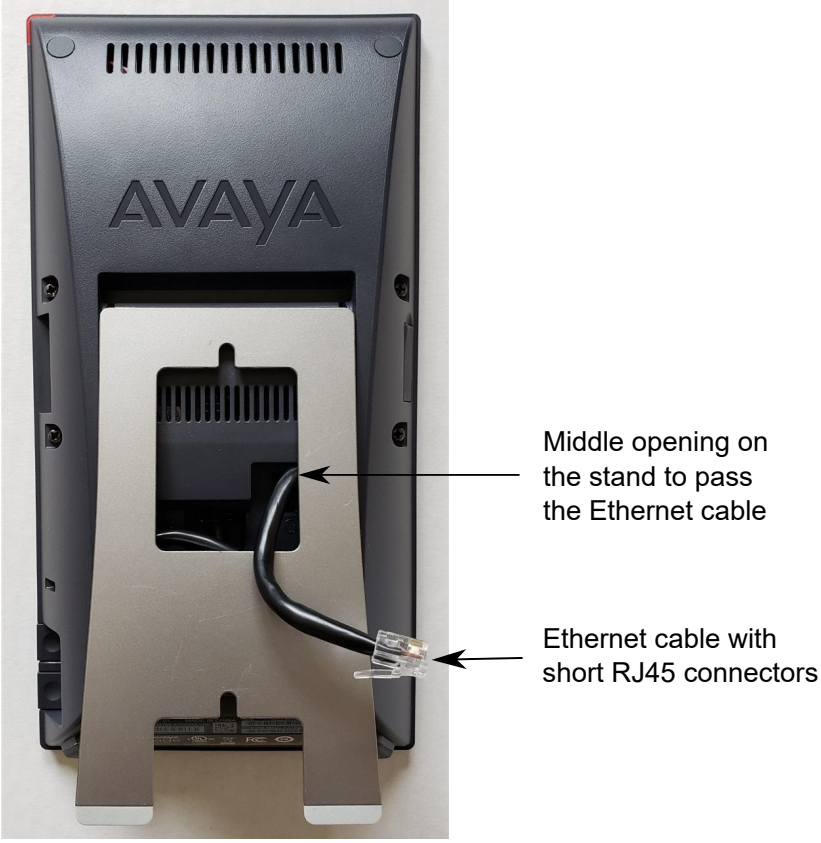
1. Attach the rubber wedge to the back of the Avaya Vantage™ device towards the base.



   The rubber wedge has a self-adhesive area that you can attach to the surface of the device. It stabilizes the wall-mounted device to prevent movement when you touch or tap the screen.

2. Plug the Ethernet cable to the LAN port on the rear panel of the device.

3. Pass the Ethernet cable through the middle gap of the stand and connect the other end to the wall jack.



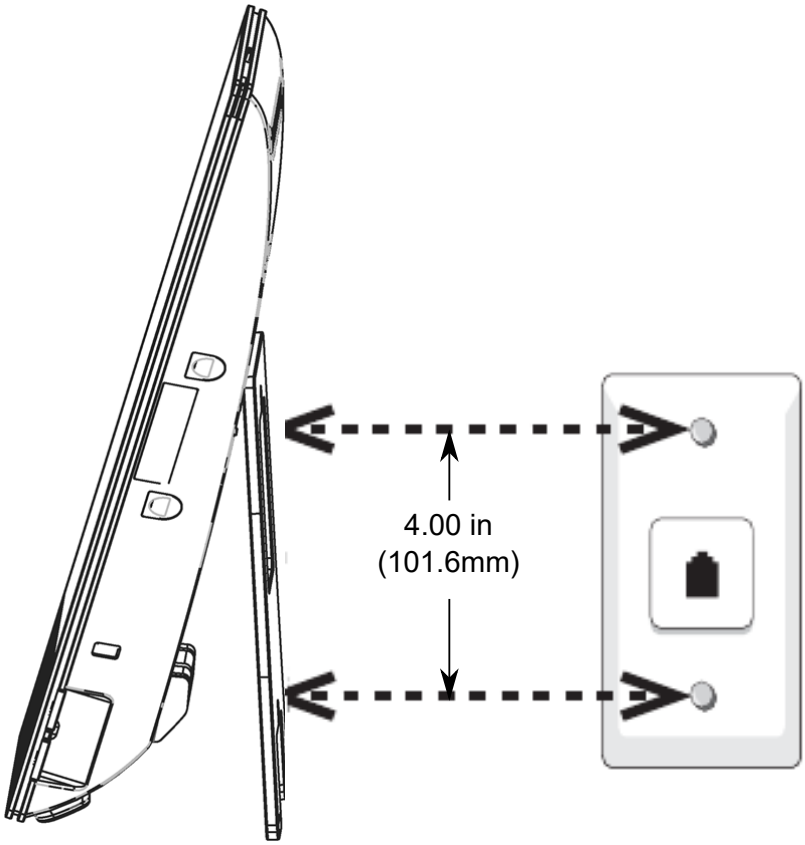
If you use a short cable as suggested, you can fold the extra length of the cable in the space between the stand and the unit.

4. **(Optional)** If you are using an external power supply or an RJ9 headset, connect the power adapter cord or the headset to the device.

   These ports are on the rear panel of the device, which are not accessible when the device is wall mounted. Therefore, carry out this step before you mount the device.

5. Close the device stand to make it rest on the rubber wedge.

6. Align the slots on the device stand with the wall plate studs and slide the device down until it attaches securely to the wall plate.



7. Place any dangling cables through the cable-access openings at the bottom of the stand and around the rubber wedge.

Wall mounting Avaya Vantage™ along with a handset cradle

About this task

You can wall mount Avaya Vantage™ using two screws or a telephone wall plate. You do not need a separate mounting kit for the device. However, you cannot directly wall mount the handset cradle using its tilt stand. You must separately purchase a cradle wall-mount kit that contains a wall-mount bracket. The part number of the cradle wall-mount kit is 700512776.

Before you begin

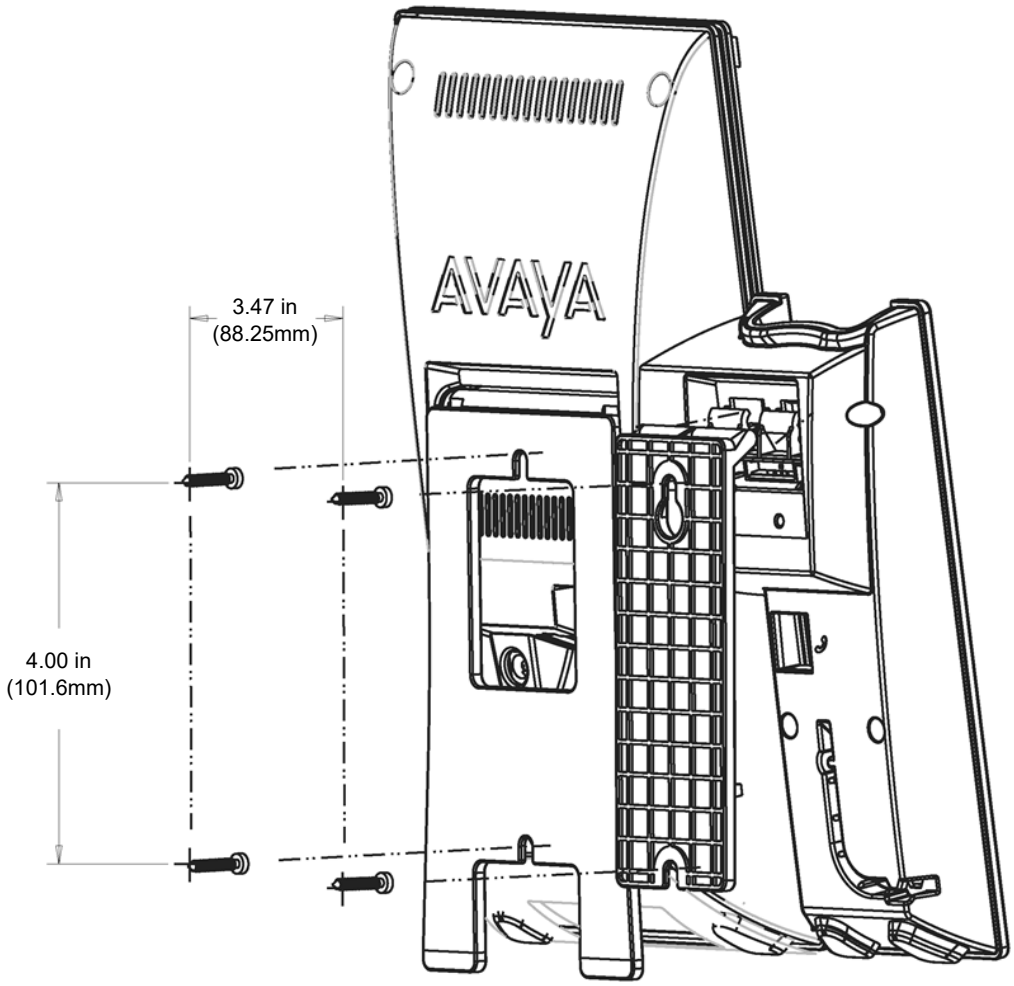
- Ensure that you are familiar with the standard processes for wall mounting an Avaya Vantage™ device using screws or a telephone wall plate. See those wall mounting procedures for the detailed steps.

- Ensure that you have the following items:
  - A cradle wall-mount kit containing a wall-mount bracket. You must order this part separately.
  - Two or four screws depending on how you are mounting your Avaya Vantage™ device.

    You need four screws if you are mounting the device using screws. If you are mounting the device on a telephone wall plate, you only need two screws for the handset cradle. The handset cradle uses the same type of wall mounting screws as the Avaya Vantage™ device.
  - Phillips-head screwdriver.
  - Pencil.
  - An Ethernet cable. If you are mounting the device on a telephone wall plate, use a short cable.

Procedure

1. Use a pencil to mark screw holes.
   - If you are using screws to mount the Avaya Vantage™ device, mark two pairs of screw holes, where each pair has two holes that are vertically spaced at 4 inches apart. Keep a horizontal distance of 3.47 inches between the two pairs of screw holes.
   - If you are mounting the device on a pre-installed telephone wall plate, mark two screw holes for the handset cradle to the left of the wall-mount plate. You must space the screw holes horizontally from each stud on the wall plate by 3.47 inches.



2. Drill holes and use a Phillips-head screwdriver to install the screws on the wall.
3. Pull the tilt stand of the handset cradle out of its socket.
4. Attach the wall-mount bracket to the handset cradle by inserting the upper tab of the bracket into the slot on the back panel of the cradle.
5. Plug the Ethernet cable to the LAN port on the rear panel of the device.
6. Close the device stand to make it rest on the rubber wedge.
7. Mount the device along with the handset securely on the screws fitted on the wall.

Chapter 4: Security configuration

The following are the key security features that are available for Avaya Vantage™:

- Device access control and user privacy through user account and device lock functionality. For more information, see Access control and user privacy on page 68.
- Complex administrator passwords to access administrator options from the **Settings** menu on the device. For more information, see Administrator password configuration on page 70.
- Certificate management for secure communication between devices, applications, and other network entities.
  - Identity certificate and trusted certificate support. Avaya Vantage™ supports up to 100 trusted certificates in either the PEM or DER format.
  - Android built-in trusted certificates that all Android applications installed on Avaya Vantage™ can use.

    According to the value set for the ENABLE_PUBLIC_CA_CERTS parameter, Device Enrollment Services, HTTP or HTTPS file downloads, PPM, SCEP over HTTPS, and Avaya Aura® Device Services use these trusted certificates.
  - No built-in Avaya product certificates including Avaya SIP Product Root CA certificate. Also, no Avaya product certificates are part of the software distribution package.

  For more information about certificate usage on Avaya Vantage™, see Certificate management on page 71.
- Support for Device Enrollment Services, which provides secure redirection of a new device to the file server. For more information, see Device Enrollment Services for secure redirection to the file server on page 78.
- Support for synchronization of time with the configured SNTP servers. For more information, see Time synchronization on page 79.
- Support for the SSH protocol to provide a secure mechanism for Avaya personnel to log in to the device remotely and perform the required operations in a secure environment. For more information, see SSH access control on page 79.
- Support for SRTP on the Avaya™ Client SDK applications. The supported Avaya™ Client SDK applications are Avaya Vantage™ Connect and Avaya IX™ Workplace Client. SRTP provides confidentiality and message authentication to media traffic going over the LAN infrastructure. With SRTP, Avaya Vantage™ can encrypt calls between two or more endpoints to prevent eavesdropping.
- Secure signaling support on the Avaya™ Client SDK application through SIP-TLS.

- TLS support for all services, such as HTTPS file downloads and SCEP over HTTPS.
- 802.1x EAP-TLS and EAP-MD5 authentication methods for Ethernet.
- Support for the following Wi-Fi security protocols: WEP, WPA, WPA2 PSK, and 802.1x, including EAP-PEAP, EAP-TLS, EAP-TTLS, and EAP-PWD with phase two authentication.
- No non-secure protocols and services, such as FTP, Telnet, TFTP, rlogin, and rsh, except for Android Debug Bridge (ADB), which is disabled by default. For more information, see Android Debug Bridge configuration on page 80.
- Support for VLAN separation mode using configuration parameters. For more information, see VLAN separation on page 81.
- Ability to disable Google Play. For more information, see Access to Google Play applications for K165 and K175 on page 132.
- Ability to disable the installation of applications from unknown sources. For more information, see Access to applications from unknown sources on page 133.
- Application download control using an XML-based configuration file. For more information, see Application download control through an XML-based configuration file on page 133.
- No root access allowed for applications. VPN tunnels for monitoring traffic are over the Wi-Fi interface only. There is no VPN support over Ethernet.
- Support for antivirus and antimalware applications.
- Android security features, such as disk encryption, remote wipe, and SELinux running in enforcing mode.
- Use of the latest Android security patches on each Avaya Vantage™ release. For more information, see Android security patches on page 86.
- Support for hardware-based random number generators.
- Support for FIPS mode, where Avaya Vantage™ uses a validated FIPS-approved cryptography library for all encryption, authentication, and random number generator algorithms. For more information, see FIPS mode on page 83.
- Ability to disable trust agents and Google Smart lock using the TRUST_AGENTS_STAT and TRUST_AGENTS_SMARTLOCK_STAT parameters.
- Ability to disable the USB port using the ENABLE_USB_GENERAL_PURPOSE parameter.
- Ability to disable wireless Bluetooth and Wi-Fi connections using the BLUETOOTHSTAT and WIFISTAT parameters.
- Ability to disable the wireless access point using the WIFIAPSTAT parameter.
- Access restrictions to parameters, so end users cannot view or configure certain parameter values from the device **Settings** menu. For more information, see Settings menu access control on page 82.

Security best practices

To maximize Avaya Vantage™ security, use the following best practices:

- Use TLS 1.2 for all services. Keep the value of TLS_VERSION as 1 to enforce TLS 1.2 usage and avoid TLS 1.0. When TLS_VERSION is set to 1, all device services, including the SIP controller and HTTPS file server, must support TLS 1.2 at minimum.
- To encrypt calls and preserve privacy, ensure that the SIP controller list is configured to work over TLS. For more information, see the SIP_CONTROLLER_LIST parameter details in Server addresses and ports on page 213.
- Enable screen lock to prevent other people from accessing user data. When you are away from your desk, you should also manually lock the device. For more information, see Access control and user privacy on page 68.
- Add password complexity to your SIP and unified login password. See Password security policies on page 69.
- Add password complexity to your administrator password. In an Avaya Aura® environment, you can use the complex password in System Manager. In the `46xxsettings.txt` file, you can configure ADMIN_PASSWORD to use only non-numeric passwords. For more information about the administrator password, see Administrator password configuration on page 70.
- Use an HTTPS file server, which requires user credentials and identity certificates. This prevents unauthorized sources from accessing the `46xxsettings.txt` file and protects the ADMIN_PASSWORD configuration.
- Configure TRUSTCERT to include the root CA of all services, especially SIP over TLS and PPM over TLS.
- Enforce certificate hostname validation by setting TLSSRVRID to 1. When this parameter value is 1, the server certificate for a service must include the correct Subject Common Name or Subject Alternative Name with the FQDN or IP address of the service.
- Keep ADB disabled unless you require it for Android application development purposes. For more information about ADB configuration, see Android Debug Bridge configuration on page 80.
- Keep SSH access disabled by setting SSH_ALLOWED to 0. You can also prevent the console port from being opened by setting AUTHCTRLSTAT to 0.
- Disable remote logging using syslog. Syslog entries are not encrypted. Set SYSLOG_ENABLED to 0 and LOGSRVR to the default setting of "". Debug logs can include user information. Debug logs have limited space, so when the log file size reaches its limit, new log entries replace old ones. You can use the CLEAR operation in administrator settings to erase all information stored on the device, including debug logs. You can also reduce the information collected internally by setting LOCAL_LOG_LEVEL to the minimum required debugging level. For more information, see Enabling verbose logging on page 163.
- Disable the installation of applications from unknown sources by setting USER_INSTALL_APPS_UNKNOWN_SOURCES to 0.
- Restrict end user access to Google Play Store by setting USER_INSTALL_APPS_GOOGLE_PLAY_STORE to 0. You can create a black or white list section in an XML-based configuration file, or block end users from installing Google Play

Store applications. For more information, see Access to Google Play applications for K165 and K175 on page 132.

- Disable Wi-Fi if you do not need it by setting WIFISTAT to 0. You can also disable Wi-Fi hotspots by setting WIFIAPSTAT to 0. When these parameter values are 0, the device user cannot configure these Wi-Fi settings through the device **Settings** menu.
- Disable Bluetooth if you do not need it by setting BLUETOOTHSTAT to 0. When this parameter value is 0, the device user cannot enable Bluetooth through the device **Settings** menu.
- Disable USB port usage by setting ENABLE_USB_GENERAL_PURPOSE to 0.
- Disable Android trust agents by setting TRUST_AGENTS_STAT to 0. When you disable trust agents, users cannot use Google and Avaya smart lock on the Avaya Vantage™ device.
- Disable Device Enrollment Services discovery if you are not using it for redirection to the file server by setting DES_STAT to 0.
- Ensure that SELinux is running in enforcing mode by setting SELINUX_MODE to the default value of 1.
- When 802.1x is enabled on Ethernet interfaces, use 802.1x EAP-TLS by setting DOT1XSTAT to 1 or 2 and DOT1XEAPS to TLS.
- Configure Avaya Vantage™ to work in VLAN separation mode to segregate network traffic between the LAN and PC ports on Avaya Vantage™ when Avaya Vantage™ is connected to a computer. For more information about VLAN separation, see Full VLAN separation on page 81.
- Enable Kiosk mode if you need to restrict end users to use only a limited set of applications. You can enforce application usage by configuring the PIN_APP parameter. For more information, see Applications to pin in Kiosk mode on page 142.
- Restrict end user access to certain configuration options in the device **Settings** menu. Use LOCKED_PREFERENCES and OBSCURE_PREFERENCES to specify the list of parameters that you want to lock or hide from end users. For more information, see Settings menu access control on page 82.
- Disable reporting to Google Analytics. Avaya Vantage™ Connect reports call statistics to Google Analytics to better understand Avaya Vantage™ Connect usage. You can disable Google Analytics by setting ANALYTICSENABLED to 0.

Access control and user privacy

To access Avaya Vantage™ telephony features, you have your own login credentials. When using Avaya Vantage™ Connect or Avaya IX™ Workplace Client on Avaya Vantage™ as the telephony application, the device supports the following two login modes:

- SIP credentials for SIP controller authentication.
- User enterprise credentials for authentication through Avaya Aura® Device Services. This option is applicable only in the Avaya Aura® environment.

Avaya Vantage™ provides lock and log out functions for user privacy. When you lock Avaya Vantage™, other users cannot unlock the device. When Avaya Vantage™ is locked, you can

receive calls or make emergency calls, but cannot access user data. If login is performed using SIP credentials, you must use the SIP password to unlock the device. If login is performed using Avaya Aura® Device Services enterprise credentials, you must use the enterprise user password to unlock the device.

You can control the locked state of the device using the following options:

- The **Screen lock** option in the **Settings** > **Security & location** menu.
- The ENABLE_PHONE_LOCK parameter.

To enable logout when the device is locked, you can set the ALLOW_LOGOUT_WHEN_LOCKED parameter. For more information, see Device lock and idle time parameters on page 294.

Note:

With IP Office, you must configure the location-specific emergency numbers in the `46xxspecials.txt` file to enable emergency calling from locked devices.

When you log out from Avaya Vantage™, the station is available for other users without access to the previous user's data. When a new user logs in, Avaya Vantage™ clears the previous user's personal data and removes all applications installed by the previous user. Applications that are installed through the PUSH_APPLICATION parameter in the settings file are not affected. When the previous user logs in again, Avaya Vantage™ restores the following information:

- The user-defined device configuration, such as language settings, which is stored on PPM or a backup server in the Avaya Aura® environment.
- The Android application data that is backed up in a personal account, such as a Google account.

Password security policies

In the SIP login password, you can use:

- Numbers: 0 – 9
- Capital letters: A – Z
- Lowercase letters: a – z
- Special characters: ~!@#$%^&*_-+=`|\(){}[]:;”’<>,.?/

In addition, the password length must be a minimum of 5 characters for the Screen lock feature on Avaya Vantage™ to work properly.

In the Avaya Aura® environment, you can configure password policies for Avaya Vantage™ using System Manager.

With IP Office, the SIP user password is required when creating a new user. For more information, see *Avaya IP Office™ Platform SIP Telephone Installation Notes*.

If you use an Exchange account on Avaya Vantage™, then security policies configured for Avaya Vantage™ must comply with the security policies configured for the Microsoft Exchange server. If

the device password does not comply with the Microsoft Exchange server policies, you might not be able to use your Exchange account. Microsoft Exchange server policies must allow the usage of numeric SIP passwords when using the SIP login method. Contact your Microsoft Exchange server vendor to obtain information about configuring password security policies.

Note:

If you use the Unified Login feature, there are no issues with the Microsoft Exchange server security policies. Avaya Vantage™ uses the Unified Login credentials to access the Exchange account.

Administrator password configuration

You must set up an administrator password to enable device administrator settings on Avaya Vantage™. Avaya Vantage™ uses the ADMIN_PASSWORD or PROCPSWD parameters to store the password and provide access to administrator options in the **Settings** menu.

- If ADMIN_PASSWORD is configured, Avaya Vantage™ uses the ADMIN_PASSWORD value and ignores the PROCPSWD value.
- If ADMIN_PASSWORD is not configured and PROCPSWD has a value different from the default, Avaya Vantage™ uses the PROCPSWD value.
- If ADMIN_PASSWORD is not configured and PROCPSWD uses the default value, you cannot access administrator options in the **Settings** menu on Avaya Vantage™.

In the Avaya Aura® environment, Avaya Vantage™ supports the complex password configured in System Manager. For a specific device location, if the complex password is configured in System Manager, then Avaya Vantage™ uses the complex password as the administrator password instead of the value defined in ADMIN_PASSWORD or PROCPSWD. This is the most secure way to configure the administrator password. If the complex password is not configured in System Manager, Avaya Vantage™ uses ADMIN_PASSWORD. Otherwise, it uses PROCPSWD. You can use the complex password to exit the kiosk mode on Avaya Vantage™.

In an IP Office environment, ADMIN_PASSWORD is added to the automatically-generated `46xxsettings.txt` file if the NUSN is set as `SET_ADMINPSWD=x` in IP Office Manager, where `x` is the administrator password.

You can change the value of ADMIN_PASSWORD and PROCPSWD using the **`SET`** command in the `46xxsettings.txt` file. You can also change the value of PROCPSWD using:

- The `name=value` pair in a DHCPACK message sent by your DHCP server.
- PPM service configuration. You cannot configure ADMIN_PASSWORD through PPM. For more information about configuring the PROCPSWD value through PPM, see *Administering Avaya Aura® Session Manager*.

Certificate management

Digital certificates are electronic documents that are used to confirm the identity of the device or application to other network entities. A number of Avaya Vantage™ applications use these certificates, which include built-in Android trusted certificates and downloaded trusted certificates.

- Avaya Vantage™ platform applications:
  - Android applications and services, such as Wi-Fi 802.1x authentication, Exchange and Google accounts, and browsers using HTTPS.
  - Avaya applications and services, such as configuration and firmware file downloads using HTTPS, SCEP over HTTPS, 802.1x EAP-TLS over Ethernet, Avaya Aura® Device Services for authenticated file server, and PPM.
- Avaya™ Client SDK-based applications: Avaya Vantage™ Connect and Avaya IX™ Workplace Client.

  Communication applications use certificates for various activities, such as SIP connectivity using SIP over TLS, PPM over TLS, and connections to Avaya Aura® Device Services servers.

Avaya Vantage™ supports installation of certificates using the following methods:

- Downloading trusted certificates using the TRUSTCERTS configuration parameter.

  TRUSTCERTS can support a list of up to 100 PEM and DER format root and intermediate trusted certificates located on the file server. You can also add trusted certificates using Android trusted certificate installation methods.

  You can configure TRUSTCERTS using the `46xxsettings.txt` file and Avaya Aura® Device Services. Configuration using Avaya Aura® Device Services gets a higher precedence than `46xxsettings.txt`. TRUSTCERTS values configured in Avaya Aura® Device Services must have the absolute URL format.
- Downloading an identity certificate as the PKCS12 file.

  Avaya Vantage™ downloads a PKCS12 file from a URL specified in the PKCS12URL configuration parameter. If the PKCS12PASSWORD configuration parameter does not contain a valid password for the PKCS12 file, Avaya Vantage™ prompts you to enter the password. If the PKCS12 file contains a trusted certificate, Avaya Vantage™ installs the PKCS12 file without the trusted certificate. You can specify the list of trusted certificates on Avaya Vantage™ only through TRUSTCERTS.

  The PKCS12 file must include the friendly name and key usage fields. Otherwise, the PKCS12 file installation on Avaya Vantage™ will not be successful.
- Generating an identity certificate using SCEP.

  Avaya Vantage™ generates and installs a new identity certificate using SCEP according to the MYCERTURL, MYCERTCN, MYCERTDN, and MYCERTCAID parameters.

  Avaya Vantage™ gives preference to the PKCS12 file over SCEP. When both the PKCS12URL and SCEP parameters are configured, Avaya Vantage™ uses the identity certificate installed using PKCS12URL.

You can review certificates installed on the Avaya Vantage™ device from the **Settings** menu:

- The USER tab in **Settings** > **Security & location** > **Encryptions & credentials** > **Trusted credentials** presents all downloaded trusted certificates. The tab also displays the identity certificate installed using SCEP or PKCS12URL.
- The SYSTEM tab in **Settings** > **Security & location** > **Encryptions & credentials** > **Trusted credentials** presents built-in Android trusted certificates.

Android built-in trusted certificates

Avaya Vantage™ supports the use of Android built-in trusted certificates by all Android applications installed on Avaya Vantage™. By default, Avaya™ Client SDK applications use built-in Android trusted certificates.

The use of Android built-in trusted certificates by some applications depends on the ENABLE_PUBLIC_CA_CERTS parameter setting. If ENABLE_PUBLIC_CA_CERTS is set to 1, then Avaya Vantage™ can use the Android built-in trusted certificates for application services such as Avaya Aura® Device Services, PPM, configuration and image file downloads, and 802.1x EAP-TLS.

The “VPN and APPS” repository contains all Android built-in trusted certificates. From Android 8.1 onwards, Avaya Vantage™ can also use the Android built-in trusted certificates for the “Wi-Fi” repository.

Downloaded trusted certificates

To store trusted certificates downloaded using TRUSTCERTS, Avaya Vantage™ uses the Android “VPN and APPS” and “Wi-Fi” repositories. These certificates are available to all Android applications.

On Avaya Vantage™, Avaya™ Client SDK applications *always* use the Android “VPN and APPS” repository that includes *all* Android built-in trusted certificates and the downloaded trusted certificates according to TRUSTCERTS. You cannot limit the Avaya™ Client SDK application to only use downloaded trusted certificates.

Note:

The TRUST_STORE parameter that you can configure to restrict Avaya IX™ Workplace Client to only use download trusted certificates is *not* applicable on Avaya Vantage™. On Avaya Vantage™, Avaya IX™ Workplace Client uses trusted certificates in the Android “VPN and APPS” repository, which includes both downloaded and Android built-in trusted certificates.

When user enterprise credentials are used for login, you must configure the root CA of the Avaya Aura® Device Services server identity certificate in TRUSTCERTS *even if* it is part of Android built-in trusted certificates. Unlike other downloaded trusted certificates, the **USER** tab in **Settings** > **Security & location** > **Encryptions & credentials** > **Trusted credentials** does not display the root CA of an Android built-in trusted certificate even if the root CA was downloaded using TRUSTCERTS.

Identity certificates generated using SCEP or downloaded using PKCS12 file

Identity certificates generated using SCEP or downloaded using PKCS12 file are stored in the Android “VPN and APPS” and “Wi-Fi” repositories. Avaya Vantage™ platform applications, the Avaya™ Client SDK application, and all Android applications can use the identity certificate generated using SCEP.

Avaya™ Client SDK applications use identity certificates for services, such as SIP connectivity, PPM, and Avaya Aura® Device Services, in the Avaya Aura® environment only. IP Office does not support client certificate validation.

Consideration while deploying Avaya Vantage™ at remote location

For a new Avaya Vantage™ device, the trusted certificate repository that is used for configuration and software file downloads using HTTPS is initially empty. As long as the trusted certificate repository remains empty, Avaya Vantage™ trusts any HTTPS file server. No initial validation of the HTTPS file server certificate occurs until trusted certificates are downloaded to the device. Therefore, Device Enrollment Services is the recommended method for new device deployments for remote users. If you do not use Device Enrollment Services, then staging is recommended to download trusted certificates to the device before sending the device to the end user.

Certificate usage by applications

The following table shows certificates that are used by different applications on Avaya Vantage™. The use of built-in Android trusted certificates by some applications depends on the ENABLE_PUBLIC_CA_CERTS parameter setting.

Application	Built-in Android trusted certificates	Downloaded trusted certificates according to the TRUSTCERTS parameter [3]	Identity certificate generated using SCEP or PKCS12 file [4]
Wi-Fi 802.1x with EAP-TLS, EAP-TTLS	Y	Y	Y
Ethernet 802.1x with EAP-TLS	Y Only when ENABLE_PUBLIC_CA_CERTS is set to 1.	Y	Y
HTTPS configuration and image files download	Y Only when ENABLE_PUBLIC_CA_CERTS is set to 1.	Y	Y
PPM	Y Only when ENABLE_PUBLIC_CA_CERTS is set to 1.	Y	Y

Table continues…

[3] Device users can install trusted certificates using Android certificate installation methods, such as through Chrome. These certificates are available to *all* Android applications.

[4] Device users can install identity certificates using Android certificate installation methods, such as through Chrome. These certificates are available to all Android applications except Avaya Breeze® Client SDK applications.

Application	Built-in Android trusted certificates	Downloaded trusted certificates according to the TRUSTCERTS parameter [3]	Identity certificate generated using SCEP or PKCS12 file [4]
SCEP over HTTPS	Y Only when ENABLE_PUBLIC_CA_CERTS is set to 1.	Y	Y
Avaya Aura® Device Services or authentication file server	Y Only when ENABLE_PUBLIC_CA_CERTS is set to 1.	Y	Y
Device Enrollment Services	Y		
Redirected file server from Device Enrollment Services	Y[5]		
Avaya Breeze® Client SDK applications	Y	Y	Y
Browser	Y	Y	Y[6]
Exchange account	Y	Y	Y
Google account	Y	Y	Y[7]
Approved third-party applications	Y	Y	Y
Non-approved third-party applications	Y	Y	N

Note:

For information about IP Office security certificates, see *Avaya IP Office™ Platform SIP Telephone Installation Notes* for Release 11.0.

[3] Device users can install trusted certificates using Android certificate installation methods, such as through Chrome. These certificates are available to *all* Android applications.

[4] Device users can install identity certificates using Android certificate installation methods, such as through Chrome. These certificates are available to all Android applications except Avaya Breeze® Client SDK applications.

[5] If Device Enrollment Services provides private CA certificates, then the private CA is used to validate the identity certificate of the redirected file server. Otherwise, the built-in Android trusted certificates are used.

[6] If the user approves, Chrome can access the device identity certificate.

[7] If the user approves, Google accounts can access the device identity certificate.

Generating a PKCS12 file with a friendly name

About this task

Use this procedure to generate a self-signed PKCS12 certificate file with a friendly name embedded.

Before you begin

Ensure that the **`openssl`** commands are available on the server console that you want to use for generating the certificate. If no OpenSSL package is found, install the latest OpenSSL package on the system.

Procedure

1. Run the following command to generate a new private key and Certificate Signing Request (CSR):

   ```
   openssl req -out CSR.csr -new -newkey rsa:2048 -nodes -keyout
   privateKey.key
   ```

   The command generates a 2048-bit RSA private key and writes it to the `privateKey.key` file. The command also generates the `CSR.csr` file that is to be signed.

2. Run the following command to generate a self-signed certificate:

   ```
   openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout
   privateKey.key -out certificate.pem
   ```

   The command output is the `certificate.pem` file, which contains the signed certificate.

3. Run the following command to generate a CSR based on an existing certificate:

   ```
   openssl x509 -x509toreq -in certificate.pem -out CSR.csr -signkey
   privateKey.key
   ```

   The command generates the `CSR.csr` file which is the CSR based on the existing `certificate.pem` file.

4. Run the following command to generate the PKCS12 file with the friendly name:

   ```
   openssl pkcs12 -export -in certificate.pem -inkey privateKey.key -
   name "friendlyName" -out cert.p12.new
   ```

   The command output is the `cert.p12.new` file, which is the new PKCS12 file with the friendly name.

5. Run the following command to read the certificate:

   ```
   openssl pkcs12 -info -nodes -in cert.p12.new
   ```

Adding a friendly name to an existing PKCS12 file

About this task

Use this procedure to add a friendly name to an existing PKCS12 file.

Procedure

1. Run the following command to extract the private key used in the certificate:

   ```
   openssl pkcs12 -in cert.p12.new -nocerts -out privateKey.key
   ```

   In this command, `cert.p12.new` is the PKCS12 file without the friendly name field.

   The command extracts the private key from the PKCS12 file to the `privateKey.key` file.

2. Run the following command to extract the identity certificate from the PKCS12 file:

   ```
   openssl pkcs12 -in cert.p12.new -clcerts -nokeys -out
   certificate.pem
   ```

   The command extracts the identity certificate from the PKCS12 file, `cert.p12.new`, to the `certificate.pem` file.

3. Run the following command to generate a new PKCS12 file with the friendly name:

   ```
   openssl pkcs12 -export -in certificate.pem -inkey privateKey.key -
   name "friendlyName" -out cert2.p12.new
   ```

   The command output is the `cert2.p12.new` file, which is the new PKCS12 file with the friendly name.

Guidelines for using a self-signed certificate

When possible, use certificates signed by a recognized CA. In a private or closed network, you can use a self-signed certificate for a service, such as file downloads from an HTTPS file server. For a successful connection, ensure that the self-signed certificate includes the following attributes:

- Basic Constraints with Subject Type set to CA.
- Key Usage with the following extensions:
  - Digital Signature
  - Non-Repudiation
  - Key Encipherment
  - Data Encipherment
  - Key Agreement
  - Certificate Signing (fc)

The following are additional recommendations for using identity certificates with Avaya Vantage™:

- Set a valid certificate expiration date and time, and configure the SNTPSRVR parameter to ensure that Avaya Vantage™ has the correct time.
- Use a certificate with a public key length of 2048 bits.
- If TLSSRVRID is set to 1, follow RFC 2818. The identity certificate for a service must include Subject Common Name or Subject Alternative Name with the FQDN or IP address that you configured for Avaya Vantage™ to access the service. For example, if you configured FILE_SERVER_URL with HTTPS and an FQDN, then include this FQDN in the Subject Alternative Name or Subject Common Name attribute of the identity certificate for the HTTPS file server.
- Do not use a wildcard character (*) in Subject Common Name and Subject Alternative Name in the identity certificate. Otherwise, Avaya Vantage™ rejects the identity certificate when opening secure TLS connection to this service. This applies to identity certificates used by Avaya Vantage™ platform services including PPM, Avaya Aura® Device Services, configuration and software file downloads using HTTPS, SCEP over HTTPS, and OCSP over HTTPS.

Use of Avaya product certificates

Avaya Vantage™ does not contain any built-in Avaya product certificates, such as the Avaya SIP Product CA certificate. These certificates are also not part of the software distribution package. You can extract and install the Avaya SIP Product CA certificate for various services that Avaya Vantage™ and the Avaya™ Client SDK application use. You can install such certificates on Avaya Vantage™ using the TRUSTCERTS parameter.

Obtaining the Avaya SIP Product CA certificate

Procedure

1. On System Manager Web Console, in the Services area, click **inventory** > **Manage Elements**.

   The system displays the Manage Elements screen.
2. Choose the Session Manager instance from the list.
3. In the **More Actions** field, click **Configure Trusted Certificates**.

   The system displays the Trusted Certificates screen.
4. Choose an Avaya SIP Product CA certificate from the list.

   For example, `trust-cert.pem`.
5. Click **Export**.

6. Save the file to a location on your system.
7. To download the CA certificate to Avaya Vantage™, do the following:
   a. Upload the CA certificate to the file server.
   b. In the `46xxsettings.txt` file, modify the TRUSTCERTS parameter value to include the CA certificate file.

Obtaining the Avaya Aura® System Manager CA certificate

About this task

If you have a server with a certificate issued by Avaya Aura® System Manager, you must distribute the Avaya Aura® System Manager CA certificate to the user's device using this procedure.

In an Avaya Aura® environment, Avaya Vantage™ can use the Avaya Aura® System Manager CA certificate for SIP, PPM, and Avaya Aura® Device Services.

Procedure

1. On System Manager Web Console, in the Services area, click **Security** > **Certificates** > **Authority**.
2. Click **Download pem file**.
3. Save the file to a location on your system.
4. To download the CA certificate to Avaya Vantage™, do the following:
   a. Upload the CA certificate to the file server.
   b. In the `46xxsettings.txt` file, modify the TRUSTCERTS parameter value to include the CA certificate file.

Device Enrollment Services for secure redirection to the file server

Device Enrollment Services provides a mechanism for Avaya endpoints to be securely authenticated and redirected to a preconfigured provisioning server. The DNS address of Device Enrollment Services is hard-coded to the device firmware. After you connect the out-of-the-box device to the network, Device Enrollment Services redirects the device to the provisioning server and then the installation procedure begins automatically.

For a fresh Avaya Vantage™ device, the trusted certificate repository that is used for configuration and software file downloads using HTTPS is initially empty. With other methods of obtaining the file server address, such as DHCP, LLDP, and manual configuration using the **Settings** menu or the installation wizard, no initial validation of the HTTPS file server certificate occurs until trusted certificates are downloaded to the device. Therefore, Device Enrollment Services is the recommended method for new device deployments for remote users. If you do not use Device

Enrollment Services, you must consider staging to download trusted certificates to the fresh device before sending the device to the end user.

Time synchronization

Avaya Vantage™ must have access to an SNTP server for time synchronization. Receiving the correct time is essential for Avaya Vantage™, especially when the device uses SIP-TLS connectivity with the SIP controller. The start time of the SIP controller identity certificate must be earlier than the current device time. Otherwise, the SIP-TLS connection fails.

The SNTPSRVR parameter provides the SNTP server addresses to Avaya Vantage™. You can configure the SNTPSRVR parameter using one of the following options, which are listed in order of precedence, from the lowest to the highest priority:

- DHCP option 42.

  If you are using DHCPv6, a `name=value` pair in DHCPv6 Reply VSI option 242.

- `46xxsettings.txt` file.
- Avaya Aura® Device Services configuration or the **Settings** menu.

  You must be in the administrator mode to configure the SNTP server addresses through the **Settings** menu.

The value of the SNTPSRVR parameter can be a comma-separated list of SNTP server addresses, which can be IPv4 or IPv6 addresses, or FQDNs. The parameter has the following default value:

```
"0.avaya.pool.ntp.org,1.avaya.pool.ntp.org,2.avaya.pool.ntp.org,3.avaya.
pool.ntp.org,129.6.15.28,132.163.97.1"
```

If you cannot reach the default SNTP servers, you must update the SNTPSRVR value to point to one or more SNTP servers that are accessible from your network.

SSH access control

Avaya Vantage™ supports remote access through SSH for troubleshooting. SSH provides a secure mechanism for Avaya personnel to log in to the device remotely and perform the required operations in a secure environment. By default, SSH access is disabled. You can control SSH access through the following:

- The SSH_ALLOWED parameter.
- The **Settings** menu on the device.

By default, SSH remote users do not have root access or access to private user data, such as:

- Private keys of digital certificates
- Authentication credentials for SIP, HTTP, 802.1X, and Exchange
- Contact and call log information
- Personal browser information, such as bookmarks, URL history, and cookies

Android Debug Bridge configuration

Avaya Vantage™ supports Android Debug Bridge (ADB). By default, ADB remains disabled on Avaya Vantage™. If ADB is required for Android application development, you can enable ADB through the **Settings** menu on the device.

You can control ADB support using the ADBSTAT parameter. You can set the parameter value to one of the following:

- 0: To completely disable ADB support. When ADBSTAT is set to 0, you cannot enable ADB through the **Settings** menu.
- 1: To be able to enable ADB through the **Settings** menu on the device.

Since ADB is a non-secure protocol, Avaya recommends that you enable ADB for Android application development purposes only. Otherwise, set ADBSTAT to 0.

Enabling or disabling ADB through the Settings menu

About this task

Use this procedure to enable or disable ADB on the Avaya Vantage™ device through the **Settings** menu. You can only enable ADB through **Settings** if ADBSTAT is set to 1.

Procedure

1. Open the **Settings** menu.
2. Tap **System** > **Developer options**.
3. **(Optional)** If **Developer options** is not available, do the following to enable developer mode:
   a. Tap **About Avaya Vantage**.
   b. Tap the **Build number** field seven times.
   c. If prompted, enter the device PIN.
4. On the Developer options screen, enable or disable ADB mode.

VLAN separation

VLANs provide a means to segregate your network into distinct groups or domains. VLANs also provide a means to prioritize network traffic into each of these distinct domains. Therefore, Avaya recommends separate VLANs for voice and data. Avaya Vantage™ devices with dual Ethernet ports have an internal network switch that can use VLANs to segregate traffic between the LAN port, the computer port, and the internal port that goes to the CPU of the device.

Avaya Vantage™ supports a full VLAN separation between data and voice VLANs. You can configure the internal network switch for VLAN separation using configuration parameters through LLDP, DHCP, and the `46xxsettings.txt` file.

Full VLAN separation

Avaya recommends a full VLAN separation between data and voice VLANs. For full VLAN separation on Avaya Vantage™, the VLAN configuration must meet the following conditions:

- VLANSEP is 1
- L2Q is 0 or 1
- L2QVLAN is not equal to 0
- PHY2VLAN is not equal to 0
- L2QVLAN is not equal to PHY2VLAN
- VLANTEST is 0 or the timer is less than 10 – 15 seconds

The Avaya Vantage™ device tries to obtain an IP address from the DHCP server on the voice VLAN. If the device gets an IP address, it sends all the tagged packets on the voice VLAN. Set the PHY2VLAN parameter to the data VLAN so that untagged packets from the computer are assigned to the data VLAN. Tagged packets from VLAN computers other than the data VLAN are blocked. PHY2VLAN is important for a *full* VLAN separation between the computer and the device VLANs.

VLAN configuration parameters

Parameter	Set to	Notes
L2Q	0, 1, or 2	Specifies 802.1Q VLAN tagging mode. Assign one of the following values: • Auto (0) or Tag (1): The device sends tagged packets on L2QVLAN until the VLANTEST time. If the DHCP server is unreachable, the device sends untagged packets. On Avaya Vantage™, the behavior is the same for both values. • Untag (2): The device sends untagged packets.

Table continues…

Parameter	Set to	Notes
L2QVLAN	Non-zero value between 1 to 4094	Specifies the 802.1Q VLAN identifier. This parameter must not have the same value as PHY2VLAN.
VLANTEST	0 to 999	Specifies the number of seconds to wait for a DHCPOFFER message reception on a non-zero VLAN. The default value is 60 seconds.
VLANSEP	1	Enables VLAN separation.
PHY2TAGS	0 or 1	Specifies whether tags are stripped from frames forwarded to the secondary Ethernet interface. • 0: VLAN tags are removed from frames forwarded to the secondary Ethernet interface. • 1: VLAN tags are not removed from frames forwarded to the secondary Ethernet interface.
PHY2VLAN	Non-zero value between 1 to 4094	Specifies the value of the 802.1Q VLAN identifier for tagged frames through the secondary Ethernet interface. This parameter must not have the same value as L2QVLAN.

Settings menu access control

You can prevent Avaya Vantage™ end users from viewing or modifying the values of certain configuration parameters through the device **Settings** menu. You can lock or hide critical parameters that you do not want the user to modify in the **Settings** menu, such as FILE_SERVER_URL, DHCP_SSON, and GROUP. To minimize cyber security risks, you can also hide parameters with IP address information, such as DNSSRVR, SNTPSRVR, and SIP_CONTROLLER_LIST.

You can use the following parameters to specify what you want to lock or hide from end users:

- LOCKED_PREFERENCES: To specify the list of parameters that you want to lock from user modification in the device **Settings** menu. The user can only view these parameter values but cannot modify them.
- OBSCURE_PREFERENCES: To specify the list of parameters that you do not want the use to see in the device **Settings** menu.

You must use the administrator password to access hidden parameters and update locked parameters from the **Settings** menu.

You can add one or more of the following parameters to LOCKED_PREFERENCES or OBSCURE_PREFERENCES as needed:

- DHCP_SSON: The site-specific option number for DHCP.
- FILE_SERVER_URL: The file server address for downloading firmware and configuration files.

- GROUP: The identifier for a set of configuration parameters in the `46xxsettings.txt` file that are specific to the user group.
- DNSSRVR: IP addresses of DNS servers.
- DOMAIN: The DNS server domain name.
- SIPDOMAIN: The SIP domain name used for SIP registration.
- SIP_CONTROLLER_LIST: Addresses of SIP proxy or registrar servers.
- IPADD: IP address, netmask, and router information of the Avaya Vantage™ device.
- L2Q and L2QVLAN: VLAN information.
- SNTPSRVR: Addresses of SNTP servers.

The following are examples of LOCKED_PREFERENCES and OBSCURE_PREFERENCES parameter settings:

```
SET OBSCURE_PREFERENCES DNSSRVR,DOMAIN,SIPDOMAIN,SIP_CONTROLLER_LIST,SNTPSRVR,IPADD
```

```
SET LOCKED_PREFERENCES DHCP_SSON,FILE_SERVER_URL,GROUP,L2Q,L2QVLAN
```

Important:

In an environment with Avaya Aura® Device Services, if the global **Lock settings** and **Obscure locked settings** options in Avaya Aura® Device Services are in the enabled state, Avaya Vantage™ ignores the preferences defined in the LOCKED_PREFERENCES and OBSCURE_PREFERENCES settings. For the LOCKED_PREFERENCES and OBSCURE_PREFERENCES settings to take effect, you must disable the global settings in Avaya Aura® Device Services.

Related links

Parameters to lock and obscure Settings menu options on page 296

FIPS mode

Avaya Vantage™ can work in FIPS-compliant mode. You can switch between FIPS and non-FIPS mode on Avaya Vantage™. When you enable FIPS mode, Avaya Vantage™ and the Avaya™ Client SDK application on the device use validated FIPS-approved cryptography libraries for encryption, authentication, and random number generator algorithms for services listed in this section.

In the FIPS mode, the Avaya Vantage™ platform and the Avaya™ Client SDK application support OpenSSL FIPS Object Module 2.0 according to NIST 2398.

Avaya Vantage™ uses its own OpenSSL FIPS Object Module cryptography library. The following services used by Avaya Vantage™ are supported in FIPS mode:

- Avaya Aura® Device Services over HTTPS in an Avaya Aura® environment.
- PPM over HTTPS in an Avaya Aura® environment.
- Configuration and software file downloads using HTTPS.

When downloading the PKCS12 file, ensure that the file is encrypted using PBE-SHA1-3DES instead of RC40 encryption. RC40 is not an approved algorithm for FIPS mode.

- SCEP over HTTP or HTTPS.

  When Avaya Vantage™ is configured to FIPS mode, ensure that CSR is encrypted using AES-256. The SCEP server must be configured to support AES-256.

- SSH.

The Avaya™ Client SDK application uses its own OpenSSL FIPS Object Module cryptography library. The following services used by the Avaya™ Client SDK application on Avaya Vantage™ are supported in FIPS mode:

- SIP
- SRTP
- SRTCP

FIPS mode configuration

Parameter configuration

You can enable or disable FIPS mode for Avaya Vantage™ using the FIPS_ENABLED parameter in the `46xxsettings.txt` file. Before enabling FIPS, perform a factory reset of the device.

You can set the FIPS_ENABLED parameter value to one of the following:

- 0: To disable FIPS mode. Services can use non FIPS-approved cryptography algorithms. This is the default value.
- 1: To enable FIPS mode. Services can use only FIPS-approved cryptography algorithms.

A change in the FIPS_ENABLED parameter value requires a device restart to activate or deactivate FIPS mode. If the device user does not respond to the reboot notification they receive, the Avaya Vantage™ device restarts automatically after 30 seconds.

After you enable FIPS, the Avaya Vantage™ device performs a self test for FIPS compliance. The FIPS self tests are performed on the Avaya Vantage™ OpenSSL and the Avaya™ Client SDK application OpenSSL.

If the self test is successful, the device works in FIPS mode. If the self test fails, Avaya Vantage™ remains logged out. If this occurs, you can disable FIPS mode from the device **Settings** menu after entering the administrator password. You can view the self test status details on the Configuration verifier screen in the **Settings** menu.

Additional FIPS compliance configuration

When you enable FIPS, perform the following additional configuration to ensure that Avaya Vantage™ remains fully FIPS-compliant:

- Run Avaya Vantage™ in Kiosk mode with only the Avaya™ Client SDK application and other Avaya-provided applications pinned on the Home screen. Configure the PIN_APP to include the following:
  - Avaya Vantage™ Kiosk application.
  - Avaya Vantage™ Connect or Avaya IX™ Workplace Client.
  - Avaya Connect Expansion Module when using Avaya Vantage™ Connect.

  Exclude third-party Android applications, which might use algorithms that are not FIPS-compliant.
- Disable Wi-Fi by setting WIFISTAT to 0.
- Disable Bluetooth by settings BLUETOOTHSTAT to 0.
- Disable the following Avaya Vantage™ services that are not FIPS-compliant:
  - 802.1x over Ethernet.
  - SLA Mon™ agent service by setting SLMSTAT to 0.
  - Device Enrollment Services by setting DES_STAT to 0 or 1.
- Install the identity certificate from the PKCS12 file or using SCEP *after* FIPS is enabled.
- Enforce use of TLS 1.2 by setting TLS_VERSION to 1.

  Ensure that services that connect with Avaya Vantage™ using TLS support TLS 1.2.
- Keep Android Debug Bridge disabled by setting ADBSTAT to 0.
- Disable Google Play by setting USER_INSTALL_APPS_GOOGLE_PLAY_STORE to 0.
- Disable installation from unknown sources by setting USER_INSTALL_APPS_UNKNOWN_SOURCES to 0.

Related links

Kiosk mode configuration checklist on page 141

Disabling FIPS mode from the Settings menu

About this task

After you enable FIPS mode, Avaya Vantage™ performs a self test for FIPS compliance. If the self-test fails, Avaya Vantage™ remains logged out. If this occurs, you can disable FIPS mode from the device **Settings** menu.

You can also set FIPS_ENABLED to 0 in the `46xxsettings.txt` file to ensure that the device does not start with FIPS mode enabled after a restart.

Before you begin

You must have the administrator password.

In an Avaya Aura® environment, if the complex password is configured in System Manager, use that password as the administrator password. If it is not available, use ADMIN_PASSWORD or PROCPSWD.

Procedure

1. Tap **Settings**.
2. In the upper-right corner of the screen, tap **Menu** > **Admin login**, and enter the administrator password.
3. Tap **System** > **Reset options** > **Clear FIPS Mode**.
4. Tap **Yes** to confirm.
5. Accept the reboot notification to restart the device with FIPS disabled.

Android security patches

Avaya Vantage™ uses the latest available Android security patch. For general information about Android security patches, see https://source.android.com/security/bulletin. You can check the Android security patch level on Avaya Vantage™ by navigating to **Settings** > **System** > **About Avaya Vantage** > **Android security patch level**.

Parameter configuration for secure installation

For secure installation, configure the following parameters.

Parameter	Recommended setting	Description
TRUSTCERTS	File names of required trusted certificates	Provides the file names of certificates to be used for authentication. It supports both root and intermediate certificates and can contain up to 100 certificate files. Avaya Vantage™ supports both PEM and DER file formats. If you configure TRUSTCERTS in the `46xxsettings.txt` file and provide relative file paths in the value, Avaya Vantage™ downloads the certificate files from the HTTP or HTTPS file server defined in FILE_SERVER_URL, HTTPSRVR, or TLSSRVR. If you define TRUSTCERTS in Avaya Aura® Device Services, you must provide absolute URLs to the certificate files.

Table continues…

Parameter	Recommended setting	Description
TLSSRVRID	1	Specifies that TLS server identification is required. Certificates installed on the servers must have a common name that matches the FQDN of the established connection. If it does not match, the connection is dropped. When set to 1, the identity certificate of Avaya Vantage™ services must have Subject Alternative name with the FQDN or IP address of the service or the FQDN or IP address of the service in the common name. If even one of the services used by Avaya Vantage™ or the Avaya™ Client SDK application has an identity certificate that does not meet the mentioned criteria, you must set TLSSRVRID to 0. Otherwise, there will be no TLS connection. Some additional considerations: • If the PPM identity certificate is signed by Avaya SIP product root CA, then TLSSRVRID must be explicitly set to 0. • Avaya™ Client SDK applications require the SIP domain in the Subject Alternative Name of the SIP controller identity certificate. If there is no such field, TLSSRVRID must be set to 0. • TLSSRVRID for Avaya IX™ Workplace Client running on any Android device has default value 0, however on Avaya Vantage™, the default is 1. For an environment where certificate validation is not required, you must configure TLSSRVRID as 0 for Avaya IX™ Workplace Client on Avaya Vantage™.
TLS_VERSION	1	Specifies the supported TLS version for all TLS connections used by Android and Avaya applications. When TLS_VERSION is set to 1, Avaya Vantage™ permits the use of TLS version 1.2 only for all services. All services that connect with Avaya Vantage™ using TLS must support TLS 1.2.
AUTH	1	Ensures usage of HTTPS file servers for configuration and software file downloads. Once AUTH is set to 1 and the device downloads the trusted certificates, the device can only download files from the HTTPS server with certificates that can be validated using the trusted certificate repository.
FILE_SERVER_URL	The address of your HTTPS file server	Assigns HTTPS or TLSRVR file servers.

Table continues…

Parameter	Recommended setting	Description
SSH_ALLOWED	0	Keeps SSH disabled.
ADBSTAT	0	Keeps ADB disabled.
ADMIN_PASSWORD	A complex password other than the default value	Enables access to administrator options in the **Settings** menu on the device using the administrator password. In an Avaya Aura® environment, the complex password configured in System Manager for the specific device location is supported and is the most secure way to configure the administrator password. If available, Avaya Vantage™ uses the complex password in System Manager. If it is not available, Avaya Vantage™ uses ADMIN_PASSWORD. Otherwise, it uses PROCPSWD.
USER_INSTALL_APPS_UNKNOWN_SOURCES	0	Keeps installation of third-party applications from unknown sources disabled. End users cannot change the permission through the **Settings** menu on the device

SCEP parameters

Parameter	Type	Default value	Description
MYCERTURL	String	Null	Specifies the URL to access the SCEP server. The device attempts to contact the server only if this parameter is set to something other than its default value.
MYCERTCN	String	$SERIALNO	Specifies the Common Name (CN) for SUBJECT in the SCEP certificate request. The values can either be $SERIALNO or $MACADDR. If the value includes the string $SERIALNO, that string will be replaced by the serial number of the phone. If the value includes the string $MACADDR, that string will be replaced by the MAC address of the phone.
MYCERTDN	String	Null	Specifies the common part of SUBJECT in the SCEP certificate request. This value defines the part of SUBJECT in a certificate request including Organizational Unit, Organization, Location, State, and Country that is common for requests from different devices.
MYCERTKEYLEN	Numeric	2048	Specifies the private key length in bits to be created in the device for certificate enrollment. The supported value is 2048.

Table continues…

Parameter	Type	Default value	Description
MYCERTREPLACE	Numeric	90	Specifies the period of the certificate's validity interval. This period is specified as a percentage. Avaya Vantage™ uses this percentage to calculate the date of the certificate replacement before its expiration. The range is from 1 to 99. When the configured period is over, Avaya Vantage™ generates a new pair of private and public keys and requests to sign the new CSR using SCEP from the CA server.
MYCERTCAID	String	CAIdentifier	Specifies the Certificate Authority Identifier. CA servers might require a specific CA Identifier string in order to accept GetCA requests. If the device works with such a CA, 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 not null, is included in a challengePassword attribute in SCEP certificate signing requests. If the value contains $SERIALNO, $SERIALNO is replaced by the value of SERIALNO. If the value contains $MACADDR, $MACADDR is replaced by the value of MACADDR without the colon separators.

PKCS12 parameters

Configure the following parameters for a PKCS12 file download to Avaya Vantage™.

Parameter	Type	Default value	Description
PKCS12URL	String	Null	Specifies the URL where a PKCS12 file containing an identity certificate is stored.
PKCS12PASSWORD	String	Null	Specifies a PKCS12 password.

Chapter 5: Data privacy controls on Avaya Vantage™ and Avaya Vantage™ Connect

Personal data is stored internally on the flash file system of Avaya Vantage™. Personal data on the file system is not externally accessible except through the following:

- SSH access, which is available to the limited-privilege craft user account for Avaya personnel through Enhanced Access Security Gateway (EASG) authentication.

  SSH access is disabled by default, but it can be enabled using an administrator password. You can also use the SSH_ALLOWED parameter in the `46xxsettings.txt` file to enable or disable SSH access. The craft and sroot access privileges are supported, and sroot provides access to `/data/app` if SELINUX_MODE is set to 0 in the `46xxsettings.txt` file or the Boot Recovery Menu (BRM).

  An Avaya authentication file can be used to enable console port for viewing user information. This file can be installed by Avaya personnel with SSH craft access. This file is limited by time and you can disable it using AUTHCTRLSTAT.

- Android Debug Bridge (ADB), if enabled.

  End users can enable ADB if ADBSTAT is set to 1.

File system content is encrypted using Android disk encryption with the 128 Advanced Encryption Standard (AES-128) protocol. When personal data is transmitted over a network, the data is encrypted with the latest protocols.

The following sections provide more information about data privacy controls that are in place for protecting personal data.

For more information about security measures that you can take to protect personal data, see Security best practices on page 67.

Avaya Vantage™ data privacy controls

Data categories containing personal data

The following are the categories of stored data and types of personal data that are contained in each data category.

User data in memory

The following personal information is available in data stored on the device's RAM:

- Remote-party phone number from calls.
- End user preferences.
- Administrator and personal configuration information including SIP login, unified login, Wi-Fi login, administrator password, personal Google account, Microsoft Exchange account, certificates, dot1x eap-tls, browsing history, download history, identity certificate, and lock password.
- Contacts retrieved from the network, including BroadSoft XSI personal and enterprise contacts.
- Contacts retrieved from the local contacts area.

User data on disk

The following personal information is saved on the device's hard disk:

- Administrator and personal configuration information including SIP login, unified login, Wi-Fi login, administrator password, personal Google account, Microsoft Exchange account, certificates, dot1x eap-tls, browsing history, download history, identity certificate, and lock password.
- Contacts retrieved from the network, including BroadSoft XSI personal and enterprise contacts.
- Contacts retrieved from the local contacts application.

User data in logs

User extension number is saved in the device logs.

User information storage

User credentials

The user's SIP registration extension and password are stored locally on the device and used for manual login and for automatic login whenever the device is started or rebooted. User enterprise credentials are also stored locally on the device and used for authentication with Avaya Aura® Device Services.

Device IP address

The device IP address is stored locally and reported to the SIP controller for information about the specific extension. In an Avaya Aura® environment, you can view the IP address using System

Manager. The device IP address can be collected by any service that the device connects to for logging purposes. Device Enrollment Services also monitors the IP address whenever the device connects to it. To enable Device Enrollment Services discovery, set DES_STAT to 2 or 3.

File server credentials

HTTP and HTTPS file server credentials are stored locally on the device and sent over the network using basic and digest authentication.

User display name

The user display name is configured in the SIP controller. For example, in an Avaya Aura® environment, you can configure it in the System Manager User configuration screen. The display name is presented to other endpoints when there is an active call.

Android account credentials and application data

Any Android account credentials, including Google and Exchange credentials, are stored locally for authentication purposes with the relevant service. Android application data, such as Google Chrome browser history, is also stored locally. You can refer to Google's data privacy policy for more information.

Wi-Fi credentials

Wi-Fi network credentials are stored locally and sent over the network for authentication.

Identity certificates

An end user can install identity certificates to the Android VPN and APPS or Wi-Fi certificate repositories. These identity certificates are used by applications and services based on user confirmation.

Personal data human access controls

User data in memory

No access to user data in memory.

User data on disk

- File system access through SSH. SSH access is only available to the limited-privilege craft user account used by Avaya personnel with EASG authentication. The craft account has limited access to the file system.

  An administrator can choose to enable or disable SSH remote access to the device.
- File system access through Android debug port when ADB is enabled.

  An administrator can choose to enable or disable ADB on the device.

User data in logs

- Through file system access.
- Through syslog server, if enabled.
- By using the **Generate debug report** option from the **Settings** menu on the device.

Personal data programmatic or API access controls

User data in memory

Data in memory is accessible through internal programmatic access. As an administrator, you can control which applications can be installed on the device. You can disable installation of external applications to block access to data in memory by external application APIs.

User data on disk

Android file system APIs have access to the file system. However, the Android application security design ensures that an application can only access its own data in the fie system.

User data in logs

None.

Encryption controls for personal data “at rest”

User data in memory

Avaya Vantage™ does not encrypt the user data on the device’s RAM.

User data on disk

Avaya Vantage™ encrypts the file system content using Android disk encryption.

User data in logs

Avaya Vantage™ encrypts the file system content using Android disk encryption.

Encryption controls for personal data “in transit”

User data in memory

Avaya Vantage™ uses standard encryption protocols for data in transit. For example, the dot1x password is sent using MD5 digest.

User data on disk

Avaya Vantage™ uses standard encryption protocols for data in transit.

User data in logs

- Syslog is not encrypted. Syslog is disabled by default on Avaya Vantage™.

  As an administrator, you can configure and control syslog for event messages on Avaya Vantage™. For more information, see Enabling verbose logging on page 163.

- Debug reports are encrypted using AES-128.

Personal data retention periods

User data in memory

The user data in memory is retained no longer than necessary to accomplish an activity or a process. For example, during an online search of enterprise contacts, search results remain in the memory until the user completes the search activity and exits the process.

User data on disk

The user data on the disk is permanent until:

- Data is overwritten.
- Another user logs in.
- You delete the application data through the **Settings** menu.
- You uninstall the application.

As an administrator, you can do the following to delete data:

- Remove all user information and restore the original factory settings by performing a factory data reset.
- Delete user-installed applications and application data.
- Clear user data in PPM in the Avaya Aura® environment. This action deletes user preferences or settings saved in PPM for Avaya Vantage™.

User data logs

Undetermined. Logs might be overwritten depending on the volume. Logs can be manually deleted.

Personal data export controls

This section provides information about restrictions and procedures available for exporting data from the device to an external system.

User data in memory

Not applicable.

User data on disk

- Local files are accessible through the Android debug port and can be copied from the Avaya Vantage™ device to a desktop.
- The SSH debug report serviceability option can be used to archive and send out all local files, including configuration and call log files, using HTTPS or TLS.

User data in logs

- Log files can be transferred through the syslog protocol. Data in syslog is not encrypted.
- The SSH debug report serviceability option can be used to archive and send out all local files, including configuration and call log files, using HTTPS.

- Debug reports can be sent to an HTTP server. While data in transit is not encrypted, the debug report is encrypted.

Personal data pseudonymization

User data in memory

None.

User data on disk

None.

User data in logs

Not applicable.

Avaya Vantage™ Connect data privacy controls

Data categories containing personal data

The following are the categories of stored data and types of personal data that is contained in each data category.

User data in memory

The following personal information is available in data stored on the device's RAM:

- Remote-party phone number from calls.
- Participant display name, roster list, and active talker from conference calls.
- End user preferences.
- Configuration information.
- Contacts retrieved from the network.
- Contacts retrieved from the local Android contacts area.

User data on disk

The following personal information is saved on the device's hard disk:

- Local call logs.
- Configuration information.
- End user preferences.
- Android user preferences.

User data in logs

The following personal information is saved in the device logs:

- User handle or email.
- SIP user name.
- Display name information from SIP messages.
- Virtual room information.
- Active talker changes.

User information storage

Call logs

User call logs are stored locally on the device. When you are logged out, call logs are stored on a server and retrieved by the device when you log in again. You can disable call logs by setting ENABLE_CALL_LOG to 0.

Contacts

User contacts are stored locally on the device. If you do not want the Contacts tab to be displayed, set ENABLE_CONTACTS to 0. If you do not want the Favorites tab to be displayed, set ENABLE_FAVORITES to 0.

User credentials

The user's SIP registration extension and password are stored on the non-persistent memory for Avaya Vantage™ Connect. The SIP credentials are used for manual login and for automatic login whenever the device is started or rebooted. User enterprise credentials are also stored on the non-persistent memory for Avaya Vantage™ Connect and are used for authentication with a unified login service. An example of a unified login service is Avaya Aura® Device Services.

Device IP address

The device IP address is stored locally and reported to the SIP controller for information about the specific extension. In an Avaya Aura® environment, you can view the IP address using System Manager. The device IP address can be collected by any service that the device connects to for logging purposes. Device Enrollment Services also monitors the IP address whenever the device connects to it. To enable Device Enrollment Services discovery, set DES_STAT to 2 or 3.

User display name

The user display name is configured in the SIP controller. For example, in an Avaya Aura® environment, you can configure it in the System Manager User configuration screen. The display name is presented to other endpoints when there is an active call.

Personal data human access controls

User data in memory

No access to user data in memory.

User data on disk

- File system access through SSH. SSH access is only available to the limited-privilege craft user account used by Avaya personnel with EASG authentication. The craft account has limited access to the file system.

  An administrator can choose to enable or disable SSH remote access to the device.
- File system access through Android debug port when ADB is enabled.

  As an administrator, you can choose to enable or disable ADB on the device.

User data in logs

- Through file system access.
- By using the **Generate debug report** option from the **Settings** menu on the device.

Personal data programmatic or API access controls

User data in memory

- Data in memory is accessible through internal programmatic access. As an administrator, you can control which applications can be installed on the device. You can disable installation of external applications to block access to data in memory by external application APIs.
- Avaya URIs are configured on the system such that when clicked from a browser or Outlook plug-in, the link opens in Avaya Vantage™ Connect.

User data on disk

Android file system APIs have access to the file system. However, the Android application security design ensures that an application can only access its own data in the fie system.

User data in logs

None.

Encryption controls for personal data “at rest”

User data in memory

Avaya Vantage™ Connect does not encrypt the user data on the device’s RAM.

User data on disk

Avaya Vantage™ encrypts the file system content using Android disk encryption.

User data in logs

Avaya Vantage™ encrypts the file system content using Android disk encryption.

Encryption controls for personal data “in transit”

User data in memory

- Avaya Vantage™ Connect uses HTTPS and TLS 1.2 to send and receive data with communication servers in the network.
- External application interfaces done through named pipe use local OS facilities and are not encrypted.

User data on disk

Avaya Vantage™ Connect uses HTTPS and TLS 1.2 to send and receive data with communication servers in the network.

User data in logs

- Avaya Vantage™ Connect uses HTTPS and TLS 1.2 to send and receive data with communication servers in the network.

  As part of Google Analytics, Avaya Vantage™ Connect collects and sends anonymous information, such as call duration.
- Syslog is not encrypted. Syslog is disabled by default on Avaya Vantage™.

  An administrator configures and controls syslog for event messages on Avaya Vantage™. For more information, see Enabling verbose logging on page 163.
- Debug reports are encrypted using AES-128.

Personal data retention periods

User data in memory

The user data in memory is retained no longer than necessary to accomplish an activity or a process. For example, during a call, a call object remains in memory. When the call ends, the object is removed from the memory, but a new `CallLog` object is created.

User data on disk

The user data on disk is permanent until:

- Data is overwritten.
- Another user logs in.
- You delete the application data through the **Settings** menu.
- You uninstall the application.

Users can delete the following information:

- Call logs and enterprise contacts.
- Application data. This action only deletes the local data, not data synced to servers.

As an administrator, you can do the following to delete data:

- Remove all user information and restore the original factory settings by performing a factory data reset.
- Delete user-installed applications and application data.
- Clear user data in PPM in the Avaya Aura® environment. This action deletes user preferences or settings saved in PPM for Avaya Vantage™.

User data logs

Undetermined. Logs might be overwritten depending on the volume. Logs can be manually deleted.

Personal data export controls

This section provides information about restrictions and procedures available for exporting data from the device to an external system.

User data in memory

Not applicable.

User data on disk

- You can copy local configuration, call logs, and log files to an external system.
- Local files are accessible through the Android debug port and can be copied from the Avaya Vantage™ device to a desktop.

User data in logs

- Local files are accessible through the Android debug port and can be copied from the Avaya Vantage™ device to a desktop.
- Syslog server, which is configured and controlled by administrators only.

Personal data pseudonymization

User data in memory

None.

User data on disk

None.

User data in logs

Not applicable.

Chapter 6: Device configuration

The following list shows the methods you can use to configure Avaya Vantage™. The methods are listed in order of precedence, from the lowest to highest priority:

- LLDP. This is the lowest priority.
- DHCP. This includes the following options:
  - Standard
  - Option 43
  - Option 242
- `46xxsettings.txt` file.
- Avaya Aura® Device Services for Avaya Aura®.

  When using Avaya Aura® Device Services for device configuration, use absolute URLs for parameters that specify file paths for downloads. For example, the TRUSTCERTS parameter value configured in Avaya Aura® Device Services must have the absolute URL format.
- PPM for Avaya Aura®.
- **Settings** menu on the device. This is the highest priority.

  Note:

  The installation wizard on Avaya Vantage™ K165 and K175 devices and Device Enrollment Services have the same priority as the **Settings** menu.

Most parameters are configurable through multiple methods. When Avaya Vantage™ receives a new parameter value, it checks precedence rules to determine whether the new value must be applied. Avaya Vantage™ changes the parameter value only if the precedence level of the new value source is higher than the precedence level of the current value source. If a source precedence level is not defined for a parameter, Avaya Vantage™ does not use the parameter values provided by that source.

For parameter descriptions, see “Appendix A: Supported configuration parameters”.

Configuration verification

To verify configuration and ensure that the device is ready to use, see Verifying device configuration on page 125.

Configuration priority for the CSDK-based telephony application

On Avaya Vantage™, Avaya IX™ Workplace Client does not support DNS service discovery through an email address followed by the retrieval of configuration data from the chosen location. Instead, Avaya Vantage™ collects the configuration data and then shares it with Avaya Vantage™ Connect or Avaya IX™ Workplace Client.

The following is the order of precedence, from lowest to highest priority, in which information is shared with the CSDK-based telephony application:

- `46xxsettings.txt` file. This is the lowest priority source.
- Avaya Aura® Device Services configuration .
- DHCP, LLDP, and the **Settings** menu for certain parameters, such as SIPDOMAIN and SIP_CONTROLLER_LIST.
- Default values enforced on certain parameters to ensure that a specific action is performed. For example, the TRUSTCERTS value is sent to the application as `""` because Avaya Vantage™ downloads the trusted certificate. The CSDK-based telephony application does not need to do this.

You can use the new Utility Server, which is embedded in Avaya Aura® Device Services, as a file server. In an environment with the Avaya Aura® Device Services Utility Server, you can choose where to configure various parameters. For example, you can configure Avaya Vantage™ platform or device parameters in the `46xxsettings.txt` file and configure CSDK-based application parameters in Avaya Aura® Device Services. Remember the priority list above. Avaya Aura® Device Services takes priority over the `46xxsettings.txt` file.

Important:

Do *not* define the PUSH_APPLICATION and ACTIVE_CSDK_BASED_PHONE_APP parameters through Avaya Aura® Device Services. Avaya Vantage™ does not collect this configuration information from Avaya Aura® Device Services.

In an environment with Avaya Aura® Utility Services as the file server, but without Avaya Aura® Device Services, all relevant parameters, including CSDK application parameters, must be configured in the `46xxsettings.txt` file.

Device configuration using LLDP

LLDP is an open standards layer 2 protocol that IP deskphones use to advertise their identity and capabilities and to receive administration from an LLDP server. LAN equipment can use LLDP to manage power, administer VLANs, and provide some administration. The transmission and reception of LLDP is specified in IEEE Std 802.1AB-2009.

Avaya Vantage™ supports transmission and reception of LLDP using Ethernet line interface. Avaya Vantage™ uses the LLDP_ENABLED parameter to determine whether LLDP is enabled on the device. You can assign one of the following values:

- 0: The transmission and reception of LLDP is disabled.
- 1: The transmission and reception of LLDP is enabled. This is the default value.
- 2: The transmission and reception of LLDP is enabled. The transmission of LLDP is started only after Avaya Vantage™ receives an LLDP frame. Avaya Vantage™ transmits the first LLDP frame within 2 seconds after the first LLDP frame is received.

After transmission is started, LLDP Data Units (LLDPDU) are transmitted every 30 seconds.

When Wi-Fi is selected as the network mode, the Ethernet ports on Avaya Vantage™ are disabled and Avaya Vantage™cannot transmit LLDP frames over Ethernet.

After receiving an LLDP frame, Avaya Vantage™ encodes the frame and stores the value of the frame in the LLDP_RCV_CONTENT parameter. Avaya Vantage™ uses the frame data only if the following conditions:

- The received frame has the destination MAC address set to the reserved group multicast address (01:80:C2:00:00:0E)
- The Ethernet protocol type is 88:CC

Avaya Vantage™ processes the value of LLDP_RCV_CONTENT every time the value of LLDP_RCV_CONTENT changes.

Initial values of parameters transmitting in LLDP frames

The following table shows the initial values of LLDP fields that are set by Avaya Vantage™ before the first LLDP frame is transmitted.

LLDP field	Value
LLDP_TTL	120
LLDP_SYSTEM_NAME	The host name sent to the DHCP server in DHCP option 12.
LLDP_BRIDGE	0
SNMP_SYS_OID	A string in the dotted-decimal character format that represents the value of the sysObjectID object in the MIB-II system group.

Table continues…

LLDP field	Value
LLDP_MAU	• 10 if the Ethernet line interface is operating at 10Mbps, half-duplex • 11 if the Ethernet line interface is operating at 10Mbps, full-duplex • 15 if the Ethernet line interface is operating at 100Mbps, half-duplex • 16 if the Ethernet line interface is operating at 100Mbps, full-duplex • 29 if the Ethernet line interface is operating at 1000Mbps, half-duplex • 30 if the Ethernet line interface is operating at 1000Mbps, full-duplex
MANUFACTURER	Avaya
POE_USED	1
POE_TYPICAL	Typical PoE power usage of the device with enabled backlight. The parameter is measured in watts.
POE_MAX	Maximum PoE power usage of the device with enabled backlight. The parameter is measured in watts. Avaya Vantage™ uses 13 for this parameter.

TLV impact on system parameter values

Avaya Vantage™ uses data transmitted in LLDP Type-Length-Value (TLV) elements to set configuration parameters. If a received LLDP frame contains a TIA LLDP-MED Capabilities TLV, then Avaya Vantage™ processes other TLVs in the frame only if the TIA LLDP-MED Capabilities TLV contains a Device Type of 0 or 4. TLVs are processed in the order that they are received.

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

Table continues…

System parameter name	TLV name	Impact
VLAN_IN_USE, L2QSIG, DSCPSIG	TIA LLDP MED Network Policy (Voice Signaling)	VLAN_IN_USE - set to the VLAN ID in the TLV. L2QSIG - Set to the Layer 2 signaling priority value in the TLV. DSCPSIG - Set to the DSCP value in the TLV (Only for IP Office and Open SIP). This TLV is ignored if: • The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0. • The Application Type is not 1 (Voice), 2 (Voice Signaling), 6 (Video Conferencing), or 8 (Video Signaling). • The Unknown Policy Flag (U) is set to 1.
VLAN_IN_USE, L2QVID, DSCPVID	TIA LLDP MED Network Policy (Video)	VLAN_IN_USE - set to the VLAN ID in the TLV. L2QVID - Set to the Layer 2 video priority value in the TLV. DSCPVID - Set to the DSCP value in the TLV (Only for IP Office and Open SIP). This TLV is ignored if: • The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0. • The Application Type is not 1 (Voice), 2 (Voice Signaling), 6 (Video Conferencing), or 8 (Video Signaling). • The Unknown Policy Flag (U) is set to 1.
SIP_CONTROLLER_LIST	Proprietary Call Server TLV	SIP_CONTROLLER_LIST will be set to the IP addresses specified in the TLV.
TLSSRVR and HTTPSRVR	Proprietary File Server TLV	FILE_SERVER_URL will be set to the IP addresses specified in the TLV.

Table continues…

System parameter name	TLV name	Impact
L2Q	Proprietary 802.1 Q Framing	If the TLV value is 1, L2Q is set to 1 (On). If the TLV value is 2, L2Q is set to 2 (Off). If the TLV value is 3, L2Q is set to 0 (Auto). A check is made as to whether a reset is necessary to obtain a new IP address due to a change in the values of the parameters L2Q or L2QVLAN. This TLV is ignored if: • The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0. • The current L2QVLAN value was set by an IEEE 802.1 VLAN name. • The current L2QVLAN value was set by a TIA LLDP MED Network Policy (Voice) TLV.

Device configuration using DHCP options

Avaya Vantage™ connects to the DHCP server during the boot up. You can use the DHCP server to provide the following information to the device:

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

You can configure the DHCP server to provision additional device and site-specific configuration parameters through various DHCP options.

Configurable DHCP options

The following options can be configured on the DHCP server:

Option	Description
Option 43	Specifies the encapsulated vendor-specific options that DHCP clients and servers use to exchange information. With option 43, you can set up your DHCP server to provide configuration for specific devices based on the vendor class identifier specified by option 60. Option 43 is processed only if the first code in the option is 1 with a value of 6889. All values are interpreted as strings of ASCII characters that are accepted with or without a null termination character. Any invalid value is ignored and the corresponding parameter value is not set.
Option 55	Specifies the parameter request list. Acceptable values are: • 1 for subnet mask. • 3 for router IP addresses. • 6 for domain name server IP address or addresses. • 7 for log server IP address or addresses. • 15 for domain name. • 26 for interface MTU. • 42 for NTP servers. • 43 for vendor-specific information. • 120 for Session Initiation Protocol (SIP) servers. • DHCP_SSON for DHCP site-specific option numbers. You can assign a value between 128 and 254.
Option 57	Specifies the maximum DHCP message size. The maximum packet size can be up to 1500 bytes. The default value is 1000.
Option 60	Specifies the vendor class identifier published by a network device. Avaya Vantage™ publishes option 60 with the value ccp.avaya.com.
Option 242	Specifies site-specific options. Option 242 is optional. If you do not configure this option, ensure that key parameters, such as the following, are configured elsewhere: • FILE_SERVER_URL • HTTPSRVR • TLSSRVR

Avaya Vantage™ sends options 55, 57, and 60 to the DHCP server to provide additional information required to configure the device.

For more information about configurable DHCP options, see RFC 2132.

Codes for option 43

The following table summarizes the supported codes for option 43 and their associated parameters. You need this information to configure DHCP option 43.

Code	Parameter
1	The first code of option 43. The value must be 6889.
2	HTTPSRVR
3	HTTPDIR
4	HTTPPORT
5	TLSSRVR
6	TLSDIR
7	TLSPORT
8	TLSSRVRID
9	L2Q
10	L2QVLAN
11	PHY1STAT
12	PHY2STAT
15	SIP_CONTROLLER_LIST
18	FILE_SERVER_URL

Parameter configuration through DHCPACK

Parameter	Set to
DHCP lease time	The value of Option 51 if received.
DHCP lease renew time	The value of Option 58 if received.
DHCP lease rebind time	The value of Option 59 if received.
DOMAIN	The value of Option 15 if received.
DNSSRVR	The value of Option 6 if received, which might be a list of IP addresses.
HTTPSRVR	The siaddr value if it is not zero. The parameter is not set if the siaddr value is zero.
IPADD	The yiaddr value.
LOGSRVR	The value of Option 7 if received, which might be a list of IP addresses.
MTU_SIZE	The value of Option 26 if received.
NETMASK	The value of Option 1 if received.
ROUTER	The value of Option 3 if received, which might be a list of IP addresses.
ROUTER_IN_USE	The giaddr value if this value not equal to zero and the current value of ROUTER_IN_USE is 0.0.0.0. In other cases, the parameter is not set.
SIP_CONTROLLER_LIST	The value of Option 120 if received, which might be a list of IP addresses or DNS names.
SNTPSRVR	The value of Option 42 if received, which might be a list of IP addresses.

DHCP site-specific options

You can specify configuration parameters for a certain Avaya Vantage™ device and assign these parameters through DHCP using site-specific options.

DHCP site-specific options allow you to specify configuration parameters for a certain Avaya Vantage™ device and assign these parameters through DHCP. A site-specific option is a sequence of comma-separated `name=value` pairs, where:

- `name` is the name of a configuration parameter. `name` is case-insensitive.
- `value` is the value that is assigned to a configuration parameter with the name matching to the value of `name`. The value of `value` is case-sensitive. To include spaces, tabs, or commas in `value`, you must use double quotes (“”).

The following is an example of a site-specific option that specifies:

- Two HTTPSRVR addresses.
- The ID of the Voice VLAN that the device must connect to.
- The ICMPDU parameter, which defines that Destination Unreachable messages must not be transmitted.

```
HTTPSRVR=“135.51.77.120,135.51.77.139”,L2QVLAN=5,ICMPDU=0
```

When specifying SIP controller addresses, you must encapsulate the value of SIP_CONTROLLER_LIST in double quotes (“”) even when you are specifying only one address. For example:

- `SIP_CONTROLLER_LIST=“145.49.103.116:5061;transport=tls”`
- `SIP_CONTROLLER_LIST=“145.49.103.116:5061;transport=tls,145.49.103.113:5061;transport=tls”`

The default DHCP option to set the site-specific configuration parameters is 242. You can also use any option ranging between 128 and 254.

Note:

When the device receives DHCP options 43 and 242, it uses option 242.

To use configuration parameters on Avaya Vantage™, you must specify the option in **DHCP Site-Specific Option Number (SSON)** on the device interface.

Site-specific configuration parameters

The following table contains a list of site-specific configuration parameters that you can define for the device.

Parameter	Description
CAPTIVE_PORTAL_SERVER	Specifies the URL of a captive portal server.
FILE_SERVER_URL	Specifies the list of file server URLs for downloading firmware and configuration files. You can enter the file server addresses in the IPv4, IPv6, or DNS name format. This parameter has higher precedence over HTTPSRVR, HTTPPORT, HTTPDIR, TLSSRVR, TLSDIR, and TLSPORT.
HTTPDIR	Specifies the path to prepend to all configurations and data files the device might request when starting up, that is, the path, relative to the root of the HTTP file server, to the directory in which the device configuration and date files are stored. The path may contain no more than 127 characters and may contain no spaces. HTTPDIR is the path for all HTTP operations. The command is `SET HTTPDIR=<path>`. In configurations where the upgrade and binary files are in the default directory on the HTTP server, do not use the `HTTPDIR=<path>`.
HTTPPORT	Destination port for HTTP requests. The default value is 80.
HTTPSRVR	IP addresses in the dot-decimal or colon-hex format, or DNS names of HTTP file servers used for downloading settings and firmware files during startup. Since the firmware files are digitally signed, TLS is not required for security. However, configuration files are not digitally signed, so it is recommended to use HTTPS servers for storing configuration and firmware files.
ICMPDU	Controls the extent to which ICMP destination unreachable messages are sent in response to messages sent to closed ports so as not to reveal information to potential hackers. The default value is 1. Use this value to send destination unreachable messages for closed ports used by the traceroute command.
ICMPRED	Controls whether ICMP Redirect messages are processed. The default value is 0, which means that redirect messages are not processed.
L2Q	802.1Q tagging mode. The default value is 0 for the automatic tagging mode.
L2QVLAN	VLAN ID of the voice VLAN. The default value is 0.
PHY1STAT	Specifies the speed and duplex settings for the primary Ethernet line interface.
PHY2STAT	Disables the secondary Ethernet line interface or specifies its speed and duplex settings.
PROCPSWD	Security string used to access local procedures. The default value is 27238.

Table continues…

Parameter	Description
SIP_CONTROLLER_LIST	SIP proxy or registrar server addresses that can be 0 to 255 characters. You can provide several IP addresses separated by commas and without spaces between entries. The default is null, which means there are no controllers. You can enter the SIP registrar addresses in the IPv4, IPv6, or DNS name format. To avoid multiple registrations to the same SIP registrar over IPv4 and IPv6, use only the DNS name format for a SIP registrar address in the list instead of using a mix of IPv4 and IPv6 addresses for the same registrar. You must encapsulate the value of SIP_CONTROLLER_LIST in double quotes (“”) even when you are specifying only one address. For example: • `SIP_CONTROLLER_LIST=“145.49.103.116:5061;transport=tls”` • `SIP_CONTROLLER_LIST=“145.49.103.116:5061;transport=tls,145.49.103.113:5061;transport=tls”`
TIMEZONE	Time zone configuration in the Olson name format. For example, `America/New_York` or `Europe/Isle_of_Man`.
TLSDIR	Used as a path name that is prepended to all file names used in HTTPS GET operations during initialization. The string length can be from 0 to 127.
TLSPORT	Destination TCP port used for requests to an HTTPS server ranging from 0 to 65535. The default value is 443, which is the standard HTTPS port.
TLSSRVR	IPv4 or IPv6 addresses, or DNS names of file servers used to download configuration and firmware files. Transport Layer Security (TLS) is used to authenticate the server and to provide encrypted data exchange between Avaya Vantage™ and the server.
USER_AUTH_FILE_SERVER_URL	Specifies the user authenticated file server URL. Enter the address using either the dot-decimal or domain name format. Add a port number, if required. In the current release, Avaya Vantage™ supports Avaya Aura® Device Services user authentication servers only.
VLANTEST	The number of seconds to wait for a DHCPOFFER on a non-zero VLAN. The default value is 60 seconds.

Device configuration using a 46xxsettings.txt settings file

You can administer Avaya Vantage™ devices centrally using the `46xxsettings.txt` settings file that Avaya provides with the devices. The settings file is a text file that resides on a file server and contains configuration parameters.

You can download the `46xxsettings.txt` file from the Avaya Support website and edit it to add your own custom settings.

Important:

In an IP Office environment, Avaya strongly recommends that you allow the IP Office system to auto-generate the settings files for devices rather than using the uploaded file. This helps to automatically adjust the settings provided to devices to match changes made in the IP Office

system configuration. For more information, see *Avaya IP Office™ Platform SIP Telephone Installation Notes*.

Customization of the settings file

The `46xxsettings.txt` settings file contains configuration parameters required to customize Avaya Vantage™ for your enterprise. You can customize the settings file to provide different parameters to devices according to various conditions, such as the following:

- Subnet of the your organization's network.
- IP address of the device.
- User group.
- Device model.

You can use the following to add your own custom settings to the `46xxsettings.txt` file:

Item	Description	Structure	Example
Tag	Specifies a string in the file. Avaya Vantage™ navigates to that string when it interprets the corresponding **Goto** command.	A single # character followed by a single space character followed by a tag name. Tag name must not include spaces. # *<TAG_NAME>*	# K175SETTINGS
Goto command	Allows Avaya Vantage™ to directly navigate to the specified tag skipping all parameters between the **Goto** command and the tag mentioned in the command.	GOTO followed by a single space character and a tag name in the following format: GOTO *<TAG_NAME>*	GOTO K175SETTINGS

Table continues…

Item	Description	Structure	Example
Conditional statement	Compares the value of a specified parameter to a some reference value. If the value of the parameter exactly matches the reference value, Avaya Vantage™ directly navigates to the tag specified in the condition. If the parameter does not exist or values do not match, Avaya Vantage™ ignores the conditional statement. Avaya Vantage™ supports the following parameters as testable parameters: • GROUP • MODEL • MODEL4 • MACADDR • IPADDR • SUBNET	`IF $<PARAMETER_NAME> SEQ <REFERENCE_VALUE> GOTO <TAG_NAME>`	`IF $MODEL4 SEQ K175 GOTO K175SETTINGS`
SET command	Assigns a value to the specified parameter. If the value is incorrect, Avaya Vantage™ does not assign it to the parameter. In this case, Avaya Vantage™ continues to use the default or previously assigned value.	`SET <PARAMETER_NAME> <PARAMETER_VALUE>`	`SET FILE_SERVER_URL http://192.168.125.161`
GET command	Avaya Vantage™ tries to download the specified settings file from the file server. If the file exists, Avaya Vantage™ downloads this file, stops to interpret the current settings file, and tries to interpret the downloaded settings file. If Avaya Vantage™ cannot download the file, it continues to interpret the current settings file.	`GET <FILE_NAME>`	`GET Settings.txt`

Table continues…

Item	Description	Structure	Example
Comment	Provides additional information about the configuration process. Avaya Vantage™ does not interpret comments.	A string started with two pound characters (`##`). `## <COMMENT>`	`## The following section contains upgrade-related parameters`

The `46xxsettings.txt` settings file must use UTF-8 encoding. All commands, parameter names, and tags are case insensitive and must use ASCII symbols.

Avaya Vantage™ handles the lines of the settings file one by one. Avaya Vantage™ interprets only one command per line. All arguments of the command must be placed on the same line as the command. To include spaces in an argument value, you must enclose the value using double quotes (“”).

User group configuration in the settings file

Use the conditional statements with the GROUP parameter to assign specific parameters or parameter values to different user groups.

The following example shows a simple settings file configuration for two user groups with the numbers 20 and 35.

```
IF $GROUP SEQ 20 GOTO CALLCENTER
IF $GROUP SEQ 35 GOTO MANAGERS
GOTO END
# CALLCENTER
## Section with parameters for Group 20 ##
SET <parameter1> <value>
SET <parameter2> <value>
SET <parameter3> <value>
GOTO END

# MANAGERS
## Section with parameters for Group 35 ##
SET <parameter1> <value>
SET <parameter2> <value>
SET <parameter3> <value>

# END
```

You can also configure GROUP from the **Settings** menu under **Network & Internet** > **More** > **Group**. In addition, Device Enrollment Services enables the configuration of FILE_SERVER_URL and GROUP for a specific Mac address or per numeric enrollment code.

After configuring user groups, you must assign a specific user group to the device. For more information, see Setting a user group for a specific configuration on page 121.

Configuring parameters in the settings file

About this task

Use this procedure to modify the settings file with appropriate values to provision the device configuration parameters.

Procedure

1. On the file server, go to the location where the `46xxsettings.txt` file is downloaded.
2. Open the `46xxsettings.txt` file in a text editor.
3. Set the required parameters as the following:

   ```
   SET <parameter_name> <parameter_value>
   ```

   For more information about the supported configuration parameters, see “Appendix A, Supported configuration parameters”.
4. Save the `46xxsettings.txt` file.

Result

On the next polling period, Avaya Vantage™ downloads the file and applies the settings.

Related links

Customization of the settings file on page 112
User group configuration in the settings file on page 114

Device configuration using Avaya Aura® Device Services

Avaya Aura® Device Services is used for retrieving configuration data when the USER_AUTH_FILE_SERVER_URL parameter points to the Avaya Aura® Device Services server. The Avaya Vantage™ device retrieves configuration data from `acs/resources/configurations` in Avaya Aura® Device Services and shares it with the CSDK-based telephony application, which can either be Avaya Vantage™ Connect or Avaya IX™ Workplace Client.

Important:

Avaya Aura® Device Services platform configuration for Android devices is not assigned to Avaya Vantage™ because Avaya Vantage™ devices are not detected as Android devices. Therefore, configuration settings in Avaya Aura® Device Services for Android devices are not sent to Avaya Vantage™.

When using Avaya Aura® Device Services for device configuration, use absolute URLs for parameters that specify file paths for downloads. For example, the TRUSTCERTS parameter value configured in Avaya Aura® Device Services must have the absolute URL format.

If the SIP user credentials are configured in Avaya Aura® Device Services, then you do not need to enter your credentials when logging in to Avaya Vantage™. Otherwise, you must enter your credentials to log in. The device can also retrieve the contact picture from Avaya Aura® Device Services to present on the Lock screen.

Do *not* define the PUSH_APPLICATION and ACTIVE_CSDK_BASED_PHONE_APP parameters through Avaya Aura® Device Services. Avaya Vantage™ does not collect this configuration information from Avaya Aura® Device Services.

Device configuration using the Settings menu on the device

Device configuration checklist

The following checklist describes task you must perform to configure Avaya Vantage™ device settings.

No.	Task	Notes	✔
1.	Configure your administration password.	Avaya Vantage™ does not provide access to Administrator mode if the default administrator password is used. See Administrator password configuration on page 70.	
2.	Ensure that you are using the Administrator mode to configure the device.	Improper modification of some settings can lead to a device malfunction. Therefore, such settings are available to administrators only. See Enabling administrator settings on the device on page 118.	
3.	Configure the file server data.	You must provide an address of a file server that is used to store software distribution packages and settings files. The file server address can be an IPv4 or IPv6 address, or an FQDN. If the file server address is configured through DHCP, LLDP, or Device Enrollment Services, you do not need to configure the file server address. See Configuring the file server address through the Settings menu on page 119.	

Table continues…

No.	Task	Notes	✔
4.	Configure the DNS server data.	You must provide the address of the DNS server used in your organization. In most cases, the DNS server address is provided through DHCP. You can also configure DNS server data statically or through the `46xxsettings.txt` file. Both the Wi-Fi and Ethernet interfaces use the configured DNS server and domain information. The option to configure DNS information specifically for each Wi-Fi network is unavailable. Therefore, if a user toggles between the Wi-Fi and Ethernet interfaces, then the configured DNS information is applicable for both interfaces. See Setting the DNS name and address on page 119.	
5.	Configure a user group.	You must specify a user group number to provide configuration parameters according to the assigned user group. See Setting a user group for a specific configuration on page 121.	
6.	Configure HTTP proxy server settings.	You must provide an address of a server that acts as a gateway between your organization's local network and other networks. If required, specify addresses that can bypass the proxy server. See Setting up an HTTP proxy and exception on page 121.	
7.	Configure SIP server settings.	You must have a SIP server to make and handle calls. Additional SIP servers can be configured to provide system survivability. If the `46xxsettings.txt` file cannot be downloaded, you can configure SIP settings through the **Settings** menu of the device See Configuring SIP server settings on page 122.	
8.	Configure a DHCP site-specific option number.	You must specify a DHCP site-specific option number to provide configuration parameters according to the assigned site-specific option. See Setting up a DHCP site-specific option number on page 123.	

Table continues…

No.	Task	Notes	✔
9.	Configure access to third party applications.	Specify which applications an end user can install. See Access to Google Play applications for K165 and K175 on page 132.	

Enabling administrator settings on the device

About this task

You can enable administrator settings on Avaya Vantage™. In the administrator mode, the device displays administrative **Settings** menu options that are unavailable to end users, such as the **SIP proxy settings** menu.

Before you begin

Get the administrator password that is set through ADMIN_PASSWORD or PROCPSWD.

In an Avaya Aura® environment, if the complex password is configured in System Manager, use that password as the administrator password. If it is not available, use ADMIN_PASSWORD or PROCPSWD.

In an IP Office environment, set ADMIN_PASSWORD using the `SET_ADMINPSWD=x` NUSN, where `x` is the password that is added to the autogenerated `46xxsettings.txt` file. For example:

```
SET_ADMINPSWD=Avaya@1234
```

Procedure

When you are logged in, do the following:

1. On the Home screen, tap **Applications**.
2. Tap **Settings**.
3. In the upper-right corner of the screen, tap **Menu** > **Admin login**.
4. Enter the administrator password, and tap **OK**.

When you are logged out, do the following:

5. On the Login screen, tap the **Settings** ( ) icon.
6. In the upper-right corner of the screen, tap **Menu** > **Admin login**.
7. Enter the administrator password, and tap **OK**.

Configuring the file server address through the Settings menu

About this task

Use this procedure to configure the file server address that the device uses for downloading software distribution packages and settings files through the **Settings** menu.

If the file server address is configured through DHCP or LLDP, you do not need to configure the file server address in the **Settings** menu of Avaya Vantage™. If Device Enrollment Services is used, then the file server redirection URL information is configured in Device Enrollment Services.

Procedure

1. On the Home screen, tap **Applications**.
2. Tap **Settings**.
3. Tap **Network & Internet** > **More** > **File Server**.
4. Enter the HTTP or HTTPS address of your file server.

   A file server URL must have one of the following format:

   - `http://hostname[:port][/path]`
   - `https://hostname[:port][/path]`

   Where:

   - `hostname` is an IPv4 or IPv6 address, or an FQDN. Encapsulate the IPv6 address in square brackets.
   - `port` is an optional port number.
   - `path` is an optional path to the directory where distribution packages and other files are stored.

   Example:

   - IPv4 address: http://192.168.1.2:80/path
   - IPv6 address: http://[2001:db8::2:1]:80/path
   - FQDN: http://hostname.domain.com:80/path

Setting the DNS name and address

About this task

As an alternative to administering DNS using DHCP, you can configure the DNS server data manually. Use this procedure to set the domain name and address of your DNS server.

Procedure

1. On the Home screen, tap **Applications**.

2. Tap **Settings**.
3. Tap **Network & Internet** > **More** > **DNS**.
4. Tap **DNS Server**.
5. Enter the IP address of the primary DNS server in **DNS Server 1**.

   You can enter an IPv4 or IPv6 address.
6. **(Optional)** If required, enter the IP address of the secondary DNS server in **DNS Server 2**.
7. Tap **OK**.
8. Tap **Domain**.
9. Enter the domain name of the DNS server.
10. Tap **OK**.

Setting the Avaya Aura® Device Services server address

About this task

Use this procedure as an alternative to administering the Avaya Aura® Device Services server address by using the `46xxsettings.txt` file. You can set the server address of Avaya Aura® Device Services if you want to use the Unified Login feature.

You must log in as an administrator to configure the Avaya Aura® Device Services information on the device through the **Settings** menu.

Note:

Avaya Aura® Device Services is supported in the Avaya Aura® environment only.

Before you begin

You must have the administrator password that is set through ADMIN_PASSWORD or PROCPSWD.

If the complex password is configured in System Manager, use that password as the administrator password. If it is not available, use ADMIN_PASSWORD or PROCPSWD.

Procedure

1. On the Home screen, tap **Applications**.
2. Tap **Settings**.
3. In the upper-right corner of the screen, tap **Menu** > **Admin login**, and enter the administrator password.
4. Tap **Network & Internet** > **More** > **Avaya Aura Device Services (AADS)**.
5. Enter the address of the Avaya Aura® Device Services server, and tap **OK**.

Related links

Administrator password configuration on page 70

Enabling administrator settings on the device on page 118

Setting a user group for a specific configuration

About this task

You can create several configuration sets and upload a specific set to the Avaya Vantage™ device according to a group identifier assigned to the device. Use this procedure to set a group identifier to the device. You can only set the group identifier using the **Settings** menu of Avaya Vantage™.

Procedure

1. On the Home screen, tap **Applications**.
2. Tap **Settings**.
3. Tap **Network & Internet** > **More** > **GROUP**.
4. Enter the group identifier.

   The group identifier must be an integer between 0 and 999 inclusively.
5. Tap **OK**.

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 exceptions to bypass the proxy server.

You can configure the HTTP proxy through the **Settings** menu only as an administrator.

Before you begin

You must have the administrator password that is set through ADMIN_PASSWORD or PROCPSWD.

In an Avaya Aura® environment, if the complex password is configured in System Manager, use that password as the administrator password. If it is not available, use ADMIN_PASSWORD or PROCPSWD.

Procedure

1. On the Home screen, tap **Applications**.
2. Tap **Settings**.
3. In the upper-right corner of the screen, tap **Menu** > **Admin login**, and enter the administrator password.
4. Tap **Network & Internet** > **More**, and tap **HTTP/S Proxy Settings**.
5. Tap **Proxy host name[:port]**.

6. Enter the HTTP proxy host name with a port number.
7. Tap **OK**.
8. (Optional) To bypass the proxy server for some specific addresses, do the following:
   a. Tap **Bypass proxy for**.
   b. Enter one or more server addresses to bypass the proxy server.

      Use commas to separate addresses.
   c. Tap **OK**.

Related links

Administrator password configuration on page 70
Enabling administrator settings on the device on page 118

Configuring SIP server settings

About this task

Use this procedure to modify the details of the defined SIP proxy servers or add a new SIP proxy server.

You can configure the SIP server and SIP domain through the **Settings** menu only as an administrator.

Before you begin

Get the administrator password that is set through ADMIN_PASSWORD or PROCPSWD.

In an Avaya Aura® environment, if the complex password is configured in System Manager, use that password as the administrator password. If it is not available, use ADMIN_PASSWORD or PROCPSWD.

Procedure

1. On the Home screen, tap **Applications**.
2. Tap **Settings**.
3. In the upper-right corner of the screen, tap **Menu** > **Admin login**, and enter the administrator password.
4. Tap **Network & Internet** > **More**, and tap **SIP Settings**.
5. Tap **SIP domain**, enter the domain name for registration, and tap **OK**.
6. To add a SIP server to the SIP servers list, do the following:
   a. Tap **SIP proxy settings**.
   b. In the upper right corner, tap **Add**.
   c. In the **SIP proxy server** field, enter the address of the SIP proxy server.

      You can use either the dotted-decimal or DNS name format.

d. In the **Transport type** field, select the appropriate transport protocol.

   In the Avaya Aura® environment, select **TLS** as the transport type. Avaya does not recommend to use TCP in the Avaya Aura® environment.

e. **(Optional)** In the **SIP port** field, enter a port number for the server to use.

   Avaya Vantage™ uses the following default port numbers:

   - 5060 for TCP
   - 5061 for TLS

f. Tap **Save**.

7. To modify the details of a SIP proxy server, tap the entry in the list, make the required changes, and tap **Save**.
8. To delete a SIP proxy server from the list, tap the entry in the list and tap **Delete**.

Related links

Enabling administrator settings on the device on page 118
Administrator password configuration on page 70

Setting up a DHCP site-specific option number

About this task

Use this procedure to assign a Site-Specific Option Number (SSON). Avaya Vantage™ uses SSON to determine which set of site-specific parameters must be downloaded from the DHCP server. This number must match a similar number option set on the DHCP server. You can set the SSON using only the **Settings** menu of Avaya Vantage™.

Procedure

1. On the Home screen, tap **Applications**.
2. Tap **Settings**.
3. Tap **Network & Internet** > **More** > **DHCP Site-Specific Option Number (SSON)**.
4. Enter the required SSON.

   The number must be in a range between 128 to 254.

Additional network configuration

Setting duplex and speed for the primary and secondary Ethernet interface

About this task

Use this procedure to modify the speed and duplex settings for the primary and secondary Ethernet line interfaces of Avaya Vantage™.

Auto negotiation is the recommended configuration setting. However, when the external switch or the network device connected to the primary or secondary Ethernet port is configured with a specific duplex and speed, then duplex and speed configuration on Avaya Vantage™ must match that configuration. You can set the 100 Mbps full-duplex option on Avaya Vantage™ and the peer at the other end. Avaya Vantage™ does not support 100 Mbps half-duplex, 10Mbps full-duplex, and 10 Mbps half-duplex configurations.

Procedure

1. From the **Settings** menu, navigate to **Network & Internet** > **Ethernet**.
2. Tap **Interfaces**.
3. Enable the administrator mode.
4. To modify the primary Ethernet interface setting, tap **Ethernet** and select one of the following:
   - **Auto**: Supports auto negotiation of speed and duplex. This is the recommended setting.
   - **100 Mbps Full**: Configures the Ethernet interface to work in full-duplex mode with a speed of 100 Mbps. Use this setting when the connected network switch is also configured for 100 Mbps full-duplex mode.

     When not using auto negotiation, both sides must be configured to use the same speed and duplex value.
5. To modify the secondary Ethernet interface setting, tap **PC Ethernet** and select one of the following:
   - **Disabled**: Disables the secondary Ethernet interface.
   - **Auto**: Supports auto negotiation of speed and duplex. This is the recommended setting.
   - **100 Mbps Full**: Configures the Ethernet interface to work in full-duplex mode with a speed of 100 Mbps.

Setting the 802.1x authentication mode

Procedure

1. Open the **Settings** menu.
2. Tap **Network & Internet** > **Ethernet**.
3. Tap **IEEE 802.1x authentication**.

   You might need to enter the administrator password.
4. **(Optional)** To change the setting for the Pass through mode, tap **Pass through mode**, and select one of the following options:
   - **Multicast pass through**: To enable multicast pass-through without proxy logoff.
   - **Multicast pass through and proxy logoff**: To enable multicast pass-through with proxy logoff.
   - **Off**: To disable multicast pass-through.

5. **(Optional)** To change the setting for the Supplicant mode, tap **Supplicant mode**, and select one of the following options:
   - **Off**: To disable the Supplicant operation.
   - **On, unicast EAPOL only**: To enable the Supplicant operation. The device responds only to received unicast Extensible Authentication Protocol over LAN (EAPOL) messages.
   - **On, unicast and multicast EAPOL**: To enable the Supplicant operation. The device responds to received unicast and multicast EAPOL messages.
6. **(Optional)** To change the Extensible Authentication Protocol (EAP) type to be used for IEEE 802.1x authentication, tap **EAP Type**, and select one of the following options:
   - **EAP-MD5**
   - **EAP-TLS**

Verifying device configuration

About this task

Use this procedure to verify that the Avaya Vantage™ device is properly configured and ready to use.

Procedure

1. Tap **Settings** > **Debugging options** > **Configuration verifier**.
2. On the Configuration verifier screen, ensure that the status of the following validations are PASS:
   - **Network Status**: Validates whether the IP address is defined and the device is connected to the network.
   - **DNS Status**: Validates whether a DNS server is configured and reachable.
   - **Date & Time Status**: Validates whether an SNTP server is configured and reachable to synchronize the device clock.
   - **File Server Status**: Validates whether the file server address is received from a configuration source and the file server is reachable.
   - **AADS Status**: Validates whether Avaya Aura® Device Services is configured and reachable.

     The Configuration verifier screen only displays this status if Avaya Aura® Device Services is configured for your setup. This field is applicable only for the Avaya Aura® environment.
   - **SIP Settings Status**: Validates whether the SIP domain and SIP controllers are configured.

     In the Avaya Aura® environment, connectivity to the PPM service is also validated.

Note:

SIP Settings Status does not validate SIP registration for the Avaya™ Client SDK telephony application.

- **Phone Application Status**: Validates whether a telephony application is defined as the active application and installed successfully.
- **Administrator Password Status**: Validates whether the administrator password is configured correctly. You can use the administrator password to access administrator options in the **Settings** menu on Avaya Vantage™.
- **FIPS Mode Status**: Indicates whether the device has passed the FIPS self test for Avaya cryptography library when FIPS mode is enabled. If the device currently supports FIPS, the detailed status displays whether any non-compliant services are running on the device. The detailed status also indicates if any identity certificate was installed on the device before FIPS mode is enabled.

  The Configuration verifier screen only displays this status if FIPS mode is enabled for your setup.
- **Camera Status**: Validates whether the camera for the device is enabled.

3. To see the details for one of the configuration items, tap the appropriate item.

   The configuration verifier displays the configuration details and status. If the status is NOTICE or FAIL, the verifier displays the possible reasons for the configuration failure. Sometimes the configuration might be correct, but verification might fail because of network connectivity issues.

   If any required configuration is missing or incorrect, modify the appropriate configuration parameter definitions.

Chapter 7: Application setup

This chapter describes how to set up applications on Avaya Vantage™. Avaya Vantage™ supports the installation of Avaya telephony applications and third-party applications.

The Avaya Vantage™ Connect and Avaya IX™ Workplace Client Android Package Kits (APKs) are bundled with the Avaya Vantage™ firmware package file and pushed automatically to the Avaya Vantage™ device. If you want to use one of these Avaya™ Client SDK applications as the active telephony application, you can set the ACTIVE_CSDK_BASED_PHONE_APP parameter in the settings file. The application you define in the parameter is installed automatically from the application APKs that are available on the device's local memory. Unless you define one of these bundled applications as the active telephony application, the application remains disabled and hidden. If a newer version of Avaya Vantage™ Connect or Avaya IX™ Workplace Client becomes available in Google Play, the Avaya Vantage™ device displays an upgrade notification.

Install and update options

You can install or update applications on Avaya Vantage™ through the following options:

- The "Push application" method. Using this method, you can initiate automatic installation, upgrade, or uninstallation of applications without end user intervention. To push an application on the device, you must upload the application APK file on the HTTP or HTTPS server and provide the path to the file in the `46xxsettings.txt` file through the PUSH_APPLICATION parameter.

  Important:

  You must specify each application only once. If you specify an application more than once, Avaya Vantage™ might not work as expected.
- Google Play. You must enable access to Google Play by using the USER_INSTALL_APPS_GOOGLE_PLAY_STORE parameter. End users can download applications from Google Play for K165 and K175. You can restrict installation of certain applications by using a configuration file.
- Third-party application stores or unknown sources. You must enable installation of applications from unknown sources by using the USER_INSTALL_APPS_UNKNOWN_SOURCES parameter. This option is disabled by default. When enabled, end users can download application APKs from common third-party application stores or other sources, such as emails or websites, to Avaya Vantage™.

With the Avaya telephony application APKs that are bundled with the Avaya Vantage™ firmware package, you do not need to use the installation options listed above. However, if you choose to install or update using these options, they take priority over the bundled APKs. If you use one of these options, Avaya Vantage™ Connect and Avaya IX™ Workplace Client will still remain hidden and disabled until one of these applications is defined as the active telephony application using ACTIVE_CSDK_BASED_PHONE_APP.

The installation options, in order of priority, for the Avaya™ Client SDK applications are:

1. Google Play store for K165 and K175 devices
2. PUSH_APPLICATION parameter
3. Bundled APKs

Automatic update of embedded Android applications

As of Release 2.0.1, on K165 and K175, the embedded Android applications get updated automatically unless you disable the auto-update option in the Google Play store.

Pushing applications onto the Avaya Vantage™ device

About this task

Use this procedure to push applications to Avaya Vantage™ without end user intervention. Through the PUSH_APPLICATION parameter, you can initiate automatic installation, upgrade, or uninstallation of applications.

Important:

While setting the PUSH_APPLICATION parameter, you must specify each application only once. If you specify an application more than once, Avaya Vantage™ might not work as expected.

Do *not* set the PUSH_APPLICATION parameter through Avaya Aura® Device Services.

Before you begin

Ensure that you have uploaded the application APK file on the HTTP or HTTPS file server or a network endpoint.

Procedure

1. Open the `46xxsettings.txt` settings file in a text editor.
2. To push a new application to the device, do one of the following depending on the scenario:
   - The settings file contains the string `SET PUSH_APPLICATION <a list of URLs>` and the list of URLs contains at least one entry: Enter a comma after the last entry, followed by the URL where the new application package file is located.
   - The settings file does *not* contain the string `SET PUSH_APPLICATION <a list of URLs>`: Add a new string with the text `SET PUSH_APPLICATION`, followed by a space and the URL where the application package file is located.

   If the application package file is stored in the root directory of the HTTP or HTTPS file server, you can provide the file name only. If the application package file is stored in a subdirectory of your HTTP or HTTPS file server, you must provide a relative path to the file. If the application package file is stored on a network endpoint, you must provide the full path to the package file.

3. To upgrade an application that was already pushed to the device, do the following:
   a. In the string `SET PUSH_APPLICATION <a list of URLs>`, locate the URL of the previous version of the application package file.
   b. Replace this URL with the URL where the latest version of the application package file is located.
4. Save the settings file.
5. Upload the settings file on the file server.

Result

In the next polling period, Avaya Vantage™ downloads the settings file and the application package and installs the application on the device.

Related links

Uninstalling a pushed application on page 129

Push command examples

The following is a simple example of using the **Push** command when the application package file is stored in the root directory of your HTTP or HTTPS file server:

```
SET PUSH_APPLICATION "com.avaya.android.vantage.basic_release_2.0.0.0.apk"
```

The following is a simple example of using the **Push** command when the application package file is stored on a network endpoint:

```
SET PUSH_APPLICATION "http://www.avaya.com/applications/download/
com.avaya.android.vantage.basic_release_2.0.0.0.apk"
```

Uninstalling a pushed application

Procedure

1. Open the `46xxsettings.txt` settings file in a text editor.
2. From the string containing the **SET PUSH_APPLICATION** command, delete the path to the application that must be uninstalled.
3. Save the settings file.
4. Upload the settings file on the file server.

Result

On the next polling period, Avaya Vantage™ uninstalls the application from the device.

Avaya telephony applications supported on Avaya Vantage™

Application	Avaya™ Client SDK application?
Avaya Vantage™ Connect	Yes
Avaya IX™ Workplace Client	Yes
Avaya Vantage™ Open	No

If you want to use an Avaya™ Client SDK telephony application, you also need to set up the ACTIVE_CSDK_BASED_PHONE_APP parameter. For more information, see Setting up an Avaya Client SDK application as the active telephony application on page 130.

Note:

In an IP Office environment, Avaya Vantage™ does not support Avaya Vantage™ Open.

Setting up an Avaya™ Client SDK application as the active telephony application

About this task

If you want to use an Avaya™ Client SDK application as the active telephony application, you must set up the ACTIVE_CSDK_BASED_PHONE_APP parameter.

The Avaya Vantage™ Connect and Avaya IX™ Workplace Client APKs are bundled in the Avaya Vantage™ firmware package and pushed automatically to the Avaya Vantage™ device. However, unless you define one of these bundled applications as the active telephony application, the application remains disabled and hidden.

For more information about acceptable values for the ACTIVE_CSDK_BASED_PHONE_APP parameter, see Package names of Avaya Client SDK applications on page 132.

Important:

Only one Avaya™ Client SDK application can be the active telephony application at a time. Therefore, ACTIVE_CSDK_BASED_PHONE_APP must contain only one package name.

Do *not* set the ACTIVE_CSDK_BASED_PHONE_APP parameter through Avaya Aura® Device Services.

Procedure

1. Open the `46xxsettings.txt` settings file in a text editor.
2. If the settings file contains the string `SET ACTIVE_CSDK_BASED_PHONE_APP <"application package name">`, replace the existing package name with the package name of the required application.

3. If the settings file does not contain the string `SET ACTIVE_CSDK_BASED_PHONE_APP <"application package name">`, do the following:

   a. Create a new string in the file below the string `SET PUSH_APPLICATION <a list of URLs>`.

   b. In the new string, enter the following:

      `SET ACTIVE_CSDK_BASED_PHONE_APP <"name of the application package">`

   For example:

```
SET PUSH_APPLICATION
com.avaya.android.vantage.basic_playstore_2.0.0.0.0406_100718_120334e.apk
SET ACTIVE_CSDK_BASED_PHONE_APP "com.avaya.android.vantage.basic"
```

4. Save and upload the settings file on the file server.

   In the next polling period, Avaya Vantage™ downloads the settings file and applies the settings accordingly.

   If not already installed, the telephony application that you define in the ACTIVE_CSDK_BASED_PHONE_APP parameter is installed using the APK available on the device's local memory. Avaya Vantage™ enables the application for the end user.

ACTIVE_CSDK_BASED_PHONE_APP parameter usage

Depending on the ACTIVE_CSDK_BASED_PHONE_APP value, Avaya Vantage™ operates in the following modes:

- If the ACTIVE_CSDK_BASED_PHONE_APP value contains the name of an Avaya™ Client SDK application, Avaya Vantage™ operates in the CSDK-based application mode. When in this mode, Avaya Vantage™ supports the Login screen and configuration sharing. For information about how to set the active Avaya™ Client SDK application in this parameter, see Setting up an Avaya Client SDK application as the active telephony application on page 130.
- If ACTIVE_CSDK_BASED_PHONE_APP is set to the default value ("""), Avaya Vantage™ does not operate in the CSDK-based application mode. In this case, some configuration parameters are not supported and some options are not available on the **Settings** menu of Avaya Vantage™. You can still configure unsupported parameters, but Avaya Vantage™ and its telephony applications will not use the configured values.

Outside of the CSDK-based application mode, user configuration backups on PPM are not supported. If a parameter supports backing up on PPM and is supported in the non CSDK application mode, then this parameter keeps the configured value unless you revert the device to its default factory settings.

Package names of Avaya™ Client SDK applications

The following table shows package names of the Avaya™ Client SDK phone applications. If you want to use an Avaya™ Client SDK phone application, you need to set the ACTIVE_CSDK_BASED_PHONE_APP parameter using the corresponding package name.

Application	Package name
Avaya IX™ Workplace Client	“com.avaya.android.flare”
Avaya Vantage™ Connect	“com.avaya.android.vantage.basic”

Parameter settings for IP Office environments

With IP Office as the file server, the `K1xxSupgrade.txt` file is automatically-generated. This file defines the ACTIVE_CSDK_BASED_PHONE_APP and PUSH_APPLICATION parameters, as shown in the following example:

```
## IPOFFICE/11.0.0.0.0 build 830 10.133.134.138 AUTOGENERATED
SET APPNAME K1xx_SIP-R1_1_0_1_3105.tar
SET ACTIVE_CSDK_BASED_PHONE_APP "com.avaya.android.vantage.basic"
SET PUSH_APPLICATION
com.avaya.android.vantage.basic_playstore_1.1.0.1.0002_280318_8334068.apk
```

Note:

If you include the line `GET 46xxsettings.txt`, then all lines after this line will be ignored. You must include such lines in the `46xxsettings.txt` file.

Access to Google Play applications for K165 and K175

For K165 and K175, Google Play is the main source of Android applications. According to your company’s policies, you can determine:

- Whether end users can install applications from Google Play. You can control access to Google Play by using the USER_INSTALL_APPS_GOOGLE_PLAY_STORE parameter in the `46xxsettings.txt` file. By default, the parameter value is set to 1 to enable installation of applications from Google Play. To disable Google Play for device users, set USER_INSTALL_APPS_GOOGLE_PLAY_STORE to 0.
- Which applications end users can install from Google Play. You can restrict installation of certain applications by using an XML-based configuration file. See Application download control through an XML-based configuration file on page 133.

Access to applications from unknown sources

On Avaya Vantage™, installation of third-party applications from unknown sources is disabled by default. End users can change the permission through the **Settings** menu. When you enable this option, end users can download application APKs from common third-party application stores and other sources, such as emails and websites, to Avaya Vantage™.

You can change this installation setting by using the USER_INSTALL_APPS_UNKNOWN_SOURCES parameter in the settings file. You can set the value of USER_INSTALL_APPS_UNKNOWN_SOURCES to one of the following:

- 0: All applications that you can use as a source for unknown applications have the permission to download and install applications from unknown sources disabled. Device users cannot change this permission status through the **Settings** menu.
- 1: All applications that you can use as a source for unknown applications have the permission to download and install applications disabled by default. Device users can change this permission status through the **Settings** menu. This is the default value of the parameter.

  You can change the permission through **Settings** > **Security & location**.
- 2: Same as when the value to set to 1.

When installation from unknown sources is enabled, Avaya Vantage™ K155 provides an application, **Application Stores Links** (), that displays links to common third-party application stores, such as F-Droid and GetJar.

Application download control through an XML-based configuration file

You can control the download of certain applications from Google Play or unknown sources by completing a black or white list section in an XML-based configuration file:

- White list: End users can install applications from the white list only. End users cannot install any applications that are not in the white list. If the white list section is configured and the list is empty, users cannot install applications from Google Play or any other sources.
- Black list: End users cannot install applications that are mentioned in the black list. If the black list is empty, users can install any third-party application from Google Play and unknown sources.

You can configure either a white list or a black list, but not both at a time.

The APPS_CONTROL_FILE parameter defines the location of the configuration file.

If the configuration file is not specified, users can install any application from Google Play and unknown sources.

Example: XML-based application control file with a white list

```
<?xml version="1.0" encoding="utf-8"?>
<applicationControl
xmlns="http://xml.avaya.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.avaya.com applicationControl.xsd">
  <allowedUserInstalledAppsUsingGooglePlayStore type="whitelist">
    <app packagename="com.avaya.android.flare" />
    <app packagename="com.avaya.android.vantage.basic" />
  </allowedUserInstalledAppsUsingGooglePlayStore>
</applicationControl>
```

Editing a black or white list

Before you begin

If you do not already have one, create an XML-based configuration file for third-party application control.

Procedure

1. Open the XML-based configuration file in a text editor.
2. To add or edit the black list, do the following:
   a. **(Optional)** If the `<allowedUserInstalledAppsUsingGooglePlayStore type="blacklist">` section is not already present in the configuration file, add the section:

      ```
      <allowedUserInstallAppsUsingGooglePlayStore type="blacklist">

      </allowedUserInstallAppsUsingGooglePlayStore>
      ```

   b. In the `<allowedUserInstalledAppsUsingGooglePlayStore type="blacklist">` section, list the applications you want to include.

      Use the following format to list the application:

      `<app packagename="<Type the package name here>" />`

      Example:

      ```
      <allowedUserInstallAppsUsingGooglePlayStore type="blacklist">
          <app packagename="com.restricted.application" />
          <app packagename="com.hacker.software" />
      </allowedUserInstallAppsUsingGooglePlayStore>
      ```

3. To add or edit the white list, do the following:
   a. **(Optional)** If the `<allowedUserInstalledAppsUsingGooglePlayStore type="whitelist">` section is not already present in the configuration file, add the section:

      ```
      <allowedUserInstalledAppsUsingGooglePlayStore type="whitelist">

      </allowedUserInstallAppsUsingGooglePlayStore>
      ```

b. In the `<allowedUserInstalledAppsUsingGooglePlayStore type="whitelist">` section, list the applications you want to include.

Use the following format:

```
<app packagename="<Type the package name here>" />
```

Example:

```
<allowedUserInstallAppsUsingGooglePlayStore type="whitelist">
    <app packagename="com.avaya.communicator" />
    <app packagename="com.avaya.android.vantage.basic" />
</allowedUserInstallAppsUsingGooglePlayStore>
```

4. Save the configuration file.
5. Upload the file on the file server.
6. In the settings file, set the APPS_CONTROL_FILE parameter to define the URL that specifies the location of the XML-based configuration file.

Result

On the next polling period, Avaya Vantage™ downloads the file and applies the settings.

Chapter 8: Emergency call configuration

To make emergency calls on Avaya Vantage™, you must configure location-specific emergency numbers.

In an Avaya Aura® environment, you can make an emergency call when you are logged out of Avaya Vantage™ or when Avaya Vantage™ is in the locked state.

In an IP Office environment, you can make an emergency call only when you are logged in to Avaya Vantage™. You can also make an emergency call from a locked device.

You can configure emergency numbers as follows:

- For Avaya Aura®: Through PPM.
- For IP Office: Through the `46xxspecials.txt` file.

You can control Lock mode for the device using one of the following:

- The ENABLE_PHONE_LOCK parameter.
- The **Screen lock** option in the **Settings** > **Security & location** menu.

Parameters for emergency numbers

The following table lists the parameters you must configure to add emergency numbers in an IP Office environment. You must set these parameters in the IP Office `46xxspecials.txt` file.

Note:

In an Avaya Aura® environment, do not configure the emergency numbers in the `46xxsettings.txt` file. Instead, configure emergency numbers in PPM through the System Manager web console. In addition, for emergency call support when you are logged out of the device, you must configure the SIP_CONTROLLER_LIST parameter using the `46xxsettings.txt` file, DHCP, LLDP, or the **Settings** menu on the device. If you only configure SIP_CONTROLLER_LIST in Avaya Aura® Device Services, emergency calls do not work as expected.

Parameter	Default value	Description
PHNEMERGNUM	Null string	Specifies the emergency number with the highest priority. Avaya Vantage™ dials this number when a user taps **Auto - dial** for an emergency call. The parameter value can contain up to 30 characters. You can use `0-9`, `*`, and `#` characters. Example: `Set PHNEMERGNUM "911"`
PHNMOREEMERGNUMS	Null string	Specifies an additional list of emergency numbers. The value of the parameter is a list of emergency numbers separated by commas without any spaces between entries. The parameter value can contain up to 100 numbers. Each number can contain up to 30 characters. You can use `0-9`, `*`, and `#` characters.

In addition, you can configure the following parameter to control whether to publish the device MAC address with all SIP messages including emergency calls:

Parameter	Default value	Description
ENABLE_PUBLISH_MAC_ADDRESS	0	Specifies whether to publish the MAC address of the Avaya Vantage™ device in all SIP signaling and PPM messages. PPM is supported in the Avaya Aura® environment only. You can assign one of the following values: • 0: SIP signaling and PPM messages do not include the MAC address of the device. • 1: SIP signaling and PPM messages include the MAC address of the device. Depending on the active network interface, the Ethernet or Wi-Fi MAC address is published in the SIP REGISTER messages. When you enable this option, a third-party location service can use the device's MAC address to determine and report the location of the device for emergency calls. For correct reporting of the Ethernet MAC address of the device in System Manager, you must set ENABLE_PUBLISH_MAC_ADDRESS to 1.

Chapter 9: Directory search configuration

Directory search and contact functionality comparison

The following table summarizes contact management on Avaya Vantage™ when deployed with different communication systems and telephony applications:

Active telephony application on Avaya Vantage™	Avaya Aura® contacts (PPM or Avaya Aura® Device Services)	IP Office directory contacts	BroadSoft directory contacts
Avaya Vantage™ Connect	Accessible through contact search: Yes You can add, edit, and delete personal enterprise contacts.	Accessible through contact search: Yes You can add, edit, and delete contacts in the personal directory.	Accessible through contact search: Yes You can add, edit, and delete contacts in the personal directory.
	Accessible from the standard Android Contacts area: No	Accessible from the standard Android Contacts area: No	Accessible from the standard Android Contacts area: Yes
Avaya IX™ Workplace Client	Accessible through contact search: Yes for enterprise contacts maintained through Avaya Aura® Device Services. Avaya IX™ Workplace Client does not support enterprise contact search when using PPM. You can add, edit, and delete personal enterprise contacts.	Accessible through contact search: Yes You can add, edit, and delete contacts in the personal directory.	Not supported.
	Accessible from the standard Android Contacts area: No		

This document is focused on Avaya Aura® and IP Office deployments. For information about BroadSoft, see *Installing and Administering Avaya Vantage™ in an Open SIP Environment*.

Avaya Aura® contact management

In an Avaya Aura® environment, you can use one of the following for the contact management functionality:

- PPM, which is a service provided by System Manager.

  Avaya™ Client SDK applications support enterprise contact search when contacts are managed through PPM.

- Avaya Aura® Device Services.

  Avaya™ Client SDK applications support enterprise contact search when contacts are managed through Avaya Aura® Device Services.

If you are using SIP credentials to log in, then contact management is performed through PPM. If you are using enterprise credentials to log in, then contact management is performed through Avaya Aura® Device Services.

You can also maintain your enterprise contacts using an LDAP directory service.

Related links

PPM configuration on page 23
Avaya Aura Device Services configuration on page 24
LDAP directory search on page 139

IP Office contact search options

In the IP Office environment, Avaya Vantage™ Connect and the standard Contacts area ( ) on the Avaya Vantage™ device support a centralized IP Office directory contact search, which includes the following:

- IP Office system contacts and hunt group contacts across a small community network
- External contacts in the LDAP, system, and HTTP directories configured on IP Office

You must define the IPO_CONTACTS_ENABLED parameter to 1 to enable IP Office contacts retrieval by the Avaya™ Client SDK application.

LDAP directory search

Avaya Vantage™ supports LDAP directory search. If your enterprise contacts are maintained using an LDAP directory service, you can configure Avaya Vantage™ to connect to the directory server and enable LDAP directory search. Avaya Vantage™ supports any directory server that supports LDAPv3.

Every application that uses the standard Android directory provider can perform an LDAP directory search. You can use Avaya Vantage™ Connect and the standard Android Contacts area available on Avaya Vantage™ to search for LDAP directory contacts.

LDAP directory search configuration

To enable or disable LDAP directory search on Avaya Vantage™, you must set the DIRENABLED_PLATFORM parameter to 1 in the `46xxsettings.txt` file. By default, this parameter is set to 0 (Disabled).

You must also define some additional parameters for Avaya Vantage™ to be able to use the LDAP directory service. For a complete list of parameters, see LDAP directory service settings on page 308.

Chapter 10: Kiosk mode configuration

You can configure Avaya Vantage™ and supported applications to work in Kiosk mode. With this mode, you can limit the applications that end users can access. Therefore, end users will only be able to access specific applications for a predetermined purpose and will not be able to access the underlying system.

For the device to work as a kiosk, you must pin the Avaya Kiosk application as a special Home screen launcher, where only predefined applications are available to the end user. To avoid getting a scroll bar, Avaya recommends that you define up to six applications to be pinned on the Home screen of the launcher.

When Avaya Vantage™ is in Kiosk mode:

- The end user cannot change the location of the application icons presented on the Home screen of the launcher.
- The device does not display a notification bar.
- The Android **Home** button is unavailable.
- Users can only use the **Back** button to return to the Home screen.

Kiosk mode configuration checklist

No.	Task	Notes	✔
1	Push the Avaya Kiosk application to the Avaya Vantage™ device.	Use the PUSH_APPLICATION parameter to install the Kiosk application on the device. You can download the Avaya Kiosk application APK file from the Downloads page for the Avaya Vantage™ firmware on the Avaya Support website. For more information about pushing applications to the device, see Pushing applications onto the Avaya Vantage device on page 128.	

Table continues…

No.	Task	Notes	✔
2	Define the Android applications to be locked on the Home screen.	Use the PIN_APP parameter to pin the required Android applications on the Home screen of the launcher. To avoid getting a scroll bar, Avaya recommends that you define up to six applications to be pinned on the Home screen. You must also include the Avaya Kiosk application package name in the PIN_APP parameter value. For a list of applications that can be pinned in Kiosk mode, see Applications to pin in Kiosk mode on page 142. To unpin, see Unpinning applications in Kiosk mode on page 143.	
3	Customize the wallpaper.	Use the CURRENT_LOGO parameter to set a wallpaper of your choice for the Home screen. Avoid using a white background image. The **Lock** icon used for exiting Kiosk mode is dimmed and difficult to see on a white background.	
4	Reboot the device.	After you complete the necessary configuration, reboot the device to apply the settings.	
5	Log on to the device and start the Kiosk mode.	This is a one-time activity. On subsequent reboots, the special Home screen for the Kiosk mode opens automatically. See Starting Kiosk mode for the first time on page 143.	

Applications to pin in Kiosk mode

Use the PIN_APP parameter in the `46xxsettings.txt` file to specify the package names of applications that you want to pin in Kiosk mode.

The package name of the Avaya Kiosk application, “com.avaya.endpoint.avayakiosk”, must be part of the PIN_APP parameter value.

The following is a list of other Avaya application packages that you can pin to the Home screen:

- “com.avaya.endpoint.login”: Login package, which provides lock and logout options in Kiosk mode.
- “com.avaya.endpoint.avayakiosk.quicklock”: Quick Lock package that provides an option to define and use a simple password for unlocking the device in Kiosk mode.
- “com.avaya.endpoint.upgrade”: Upgrade package, which enables firmware upgrades.
- “com.avaya.contexthelp”: Help package, which provides access to online help for the Avaya Vantage™ device.

- “com.avaya.endpoint.cleanmode”: Clean mode package. You can temporarily disable the device touch screen for 30 seconds to avoid activating any function while you wipe the screen.
- One of the following CSDK telephony applications:
  - “com.avaya.android.flare”: Avaya IX™ Workplace Client.
  - “com.avaya.android.vantage.basic”: Avaya Vantage™ Connect.
- “com.avaya.vantageremote”: Avaya Connect Expansion Module, which you can use with Avaya Vantage™ Connect in an Avaya Aura® environment.
- “com.avaya.endpoint.avayavoiceassistant”: Voice Assistant for Avaya Vantage™, which is available for K175 devices.

You can also pin other Android applications. For example, “com.android.chrome” provides access to the Google Chrome browser.

Changes to the PIN_APP parameter value take effect on the next polling period or after you restart the Avaya Vantage™ device.

The following is an example of the parameter setting:

```
SET PIN_APP
“com.avaya.endpoint.avayakiosk,com.avaya.android.vantage.basic,com.avaya.endpoint.avayak
iosk.quicklock,com.android.chrome,com.avaya.endpoint.login,com.avaya.endpoint.avayavoice
assistant,com.android.calculator2”
```

Unpinning applications in Kiosk mode

About this task

Only unpin applications that are in an idle state, and not while an active call is in progress.

Procedure

In the `46xxsettings.txt` file, remove the package name of the application you want to unpin from the PIN_APP parameter value.

Changes to the PIN_APP parameter value take effect on the next polling period or after you restart the Avaya Vantage™ device.

Starting Kiosk mode for the first time

Before you begin

- Complete the configuration tasks. See Kiosk mode configuration checklist on page 141.
- Reboot the Avaya Vantage™ device.

Procedure

1. Log on to the device using the SIP user credentials.

2. On the Home screen, tap the Avaya Kiosk application icon.

   The device displays the special Home screen of the launcher and the icons for the pinned applications.

   On subsequent reboots, the special Home screen opens automatically.

Exiting the Kiosk mode

About this task

Use this procedure to exit the Kiosk mode and access the device normally.

Procedure

1. Tap the **Lock** icon located at the bottom-right side of the screen.
2. Enter the administrator password that is configured in ADMIN_PASSWORD or PROCPSWD, and then tap **OK**.

   In an Avaya Aura® environment, if the complex password is configured in System Manager, use that password as the administrator password. If it is not available, use ADMIN_PASSWORD or PROCPSWD.
3. To exit Kiosk mode, swipe up and tap **Home**.

Chapter 11: Device start up, screen saver, and lock configuration

Device start-up configuration

You can minimize audio and visual notifications when Avaya Vantage™ turns on or restarts. For example, when resetting devices remotely in a hotel at night, you can disable audio and visual notifications to avoid disturbing guests. You can control audio and visual notifications with the following configuration parameters in the `46xxsettings.txt` file:

- BRANDING_VOLUME: You can disable the playback of the Avaya branding tone by setting the parameter value to 0. Otherwise, the device plays this tone when the login is successful after the device restarts.
- DARK_BOOTUP: You can turn off the device backlight by setting the parameter value to 1. The device does not display start-up screens when the backlight is off.

  The backlight turns on if you pick up the handset, touch the screen or hard key buttons, or when there is an incoming call.

Related links

General phone functionality settings on page 198
Device UI related settings on page 201

Login screen configuration

You can control whether to preserve login credentials on the Avaya Vantage™ Login screen after the user logs out or taps **Cancel** during a login operation. You can control this behavior through the following parameters in the `46xxsettings.txt` file:

- SHOW_LAST_EXTENSION: To preserve the SIP extension or unified login ID on the Login screen after you log out or tap **Cancel** during a login operation, set this parameter value to 1.
- PRESERVE_LOGIN_PASSWORD: To preserve the SIP or unified login password on the Login screen after you tap **Cancel** during a login operation, set this parameter value to 1.

Related links

Login screen specific parameters on page 293

Screen saver configuration

You can centrally manage screen saver behavior on Avaya Vantage™ devices through configuration parameters. You can push screen saver images to Avaya Vantage™ and choose which screen saver the device displays. You can also control whether device users can set up a screen saver of their choice locally from the device.

Using configuration parameters, you can:

- Control whether the **Screen Saver** option is enabled in the **Settings** menu for device users.
- Push a set of custom screen saver images to Avaya Vantage™.
- Set one of the custom images as the screen saver.

  When the **Screen Saver** option is enabled in the device **Settings** menu, device users can replace this custom screen saver with a screen saver of their choice.
- Configure the device sleep time, after which the device displays the screen saver.
- Control whether device users can change the device sleep time through the **Settings** menu.

Parameters for screen saver configuration

To manage screen saver behavior on Avaya Vantage™, configure the following parameters.

In an Avaya Aura® environment, you can set up the parameters through the `46xxsettings.txt` file or Avaya Aura® Device Services. In an IP Office environment, use the `46xxspecials.txt` file, which is called from the automatically generated `46xxsettings.txt` file.

Parameter	Default value	Description
SCREENSAVER_IMAGE_SELECTABLE	1	Specifies whether device users can set up a screen saver of their choice locally from the device **Settings** menu. You can assign one of the following values: • 0: To disable the screen saver selection option for device users. • 1: To enable the screen saver selection option for device users.

Table continues…

Parameter	Default value	Description
SCREENSAVER_IMAGE	“”	Specifies a list of custom screen saver images to be downloaded to Avaya Vantage™. The parameter value can be a comma-separated list of screen saver image URLs. The list entries are separated by commas without any intervening spaces. You can specify a URL using the absolute or relative format. For the relative format, the origin is the directory specified by FILE_SERVER_URL. Avaya Vantage™ supports the following file types: PNG, JPG (JPEG), GIF, and BMP. GIF is presented without animation. Use an image that fits the entire device screen. • For K175 devices, the screen is 8 inches with a resolution of 800 x 1280 (width x height) pixels. • For K155 devices, the screen is 5 inches with a resolution of 1280 x 720 (width x height) pixels. Example: `SET SCREENSAVER_IMAGE “redballoon.jpg,https://123.234.5.6/blueballoon.jpg”`
SCREENSAVER_IMAGE_DISPLAY	“”	Specifies the custom screen saver image to be displayed on Avaya Vantage™. The image file name must be the same as one of the file names you listed in SCREENSAVER_IMAGE. Example: `SET SCREENSAVER_IMAGE_DISPLAY redballoon.jpg` If you set SCREENSAVER_IMAGE_SELECTABLE to 1, then device users can override this custom screen saver with a screen saver of their choice through the device **Settings** menu. If you do not set a screen saver image or set the wrong file name in this parameter, device users see a black screen as the custom screen saver.
BACKLIGHT_SELECTABLE	1	Specifies whether the device sleep time is determined by you, as the administrator, or through user configuration. After the device is idle for the specified sleep time, the device display backlight is turned off. You can assign one of the following values: • 0: To obtain the device idle time value from the BAKLIGHTOFF parameter you set in the `46xxsettings.txt` file. • 1: To enable the user to set the idle time value through the **Sleep** option in the **Settings** > **Display** menu.

Table continues…

Parameter	Default value	Description
BAKLIGHTOFF	60	Specifies the device idle time in minutes, after which the device turns off the display backlight or activates the screen saver. The range is from 0 to 999. This parameter is only applicable when BACKLIGHT_SELECTABLE is set to 0.

Lock screen and idle time configuration

You can centrally manage the Lock screen behavior on Avaya Vantage™ through configuration parameters in the `46xxsettings.txt` file. You can enable the lock screen and set the idle time after which the device is locked automatically. You can also control whether users can log out from the Lock screen.

Related links

Device lock and idle time parameters on page 294

Chapter 12: Avaya Vantage™ Connect configuration

You can configure and control features that device users can access on Avaya Vantage™ Connect. You can configure most feature options using parameters in the `46xxsettings.txt` file. In addition, you can enable the use of Avaya Connect Expansion Module in conjunction with Avaya Vantage™ Connect to provide advanced telephony features to device users.

Hot dialing configuration

As an administrator, you can configure hot dialing on Avaya Vantage™ Connect to use the Avaya Vantage™ device as a hotline station. When hot dialing is enabled, Avaya Vantage™ Connect automatically places a call to the configured phone number when the device goes off-hook.

For example, you can enable hot dialing for devices kept at lobbies or security gates for guests. So when a guest lifts the handset, a call automatically goes to the reception or security desk.

When hot dialing is enabled, device users can answer incoming calls to the hotline station, but access to other features is limited. You cannot:

- Dial any other phone numbers or extensions.
- Access application settings.
- Access the Join meeting feature.

By defining configuration parameters, you can set the hotline number and the outgoing call type. You can control whether users of the hotline station can access call hold, conferencing, and transfer capabilities. You can also limit the user's access to the Favorites, Contacts, and Call History tabs.

Hot dialing configuration checklist

Use the parameters in the `46xxsettings.txt` file to configure hot dialing. This checklist summarizes the hot dialing configuration tasks.

No.	Task	Descriptions	✔
1	Configure the hotline number.	To enable hot dialing, define the HOTLINE parameter in the settings file with the phone number to be dialed automatically by Avaya Vantage™ Connect. The default value of the HOTLINE parameter is null (“”). Use this default value if you want hot dialing to remain disabled. A valid phone number or extension can contain up to 30 dialable characters that can include: 0 to 9, *, and #. To autodial a number with a password, you can include a comma between the phone number and the password in the parameter value. For example: `SET HOTLINE “<extension>,<password>#”`	
2	Define whether the outgoing call to the hotline number will be an audio or video call.	Use the HOTLINE_CALL_TYPE parameter to define the outgoing call type. You can set one of the following values: • 0: Audio call. This is the default setting. • 1: Video call.	
3	Customize a message to be displayed on the application screen.	Use the HOTLINE_ADMIN_MESSAGE parameter to customize the message to be displayed on the Home screen of Avaya Vantage™ Connect when hot dialing is enabled. The default message is `Lift handset to place a call to Hotline number.` On K175, the message length can be a maximum of 255 characters. On K155, the maximum length is 68 characters.	

Table continues…

No.	Task	Descriptions	✔
4	As required, limit user access to Avaya Vantage™ Connect features, such as hold and transfer call.	Use the following parameters to limit user access to other Avaya Vantage™ Connect features: • HOLDSTAT: Set to 0 to disable call holding. Set CCBTNSTAT to 0. • CONFSTAT: Set to 0 to disable conferencing and call merging. Set CCBTNSTAT to 0. • XFERSTAT: Set to 0 to disable call transfer. Set CCBTNSTAT to 0. • ENABLE_FAVORITES: Set to 0 to hide the Favorites tab. • ENABLE_CONTACTS: Set to 0 to hide the Contacts tab. • ENABLE_CALL_LOG: Set to 0 to hide the Call History tab. • ENABLE_JOIN_EQUINOX_MEETING: Set to 0 to hide the **Join Meeting** icon on the Dial pad tab.	
5	Pin the Avaya Vantage™ Connect application to the device Home screen.	To prevent the user from accessing other applications and device options, such as device settings and the logout option, lock the Avaya Vantage™ Connect application to the device Home screen by setting the PIN_APP parameter to `"com.avaya.android.vantage.basic"`.	
6	If required, limit user access to voice mail messages.	Modify the voice mail access permission for the SIP user account used for logging in to the hotline station. You can configure voice mail access permission as follows: • In an Avaya Aura® environment, on System Manager. • In an IP Office environment, on IP Office Manager.	

For more information about the configuration parameters, see Avaya Vantage Connect parameters on page 261.

Parameter configuration example for hot dialing

The following is an example of hot dialing configuration in the `46xxsettings.txt` file. In this example, the Favorites, Contacts, and Call History tabs are hidden, and the hold, conferencing, and transfer features are disabled.

```
SET HOTLINE "68000987"
SET HOTLINE_CALL_TYPE 1
SET HOTLINE_ADMIN_MESSAGE "Lift the handset to place a call to the Front desk
connoisseur."
```

```
SET ENABLE_CALL_LOG 0
SET ENABLE_CONTACTS 0
SET ENABLE_FAVORITES 0
SET ENABLE_REDIAL 0

SET HOLDSTAT 0
SET CONFSTAT 0
SET XFERSTAT 0
SET CCBTNSTAT 0

SET PIN_APP "com.avaya.android.vantage.basic"
```

Microsoft Exchange Calendar integration with Avaya Vantage™ Connect

For Avaya Vantage™ Connect to access Microsoft Exchange Calendar information, you must enable Exchange Web Services (EWS). You can also control the display of the Calendar tab on Avaya Vantage™ Connect.

Avaya Vantage™ Connect can interoperate with the following Microsoft Exchange server versions:

- 2013
- 2016
- Office 365

Parameters for calendar configuration

To integrate Microsoft Exchange Calendar with Avaya Vantage™ Connect, configure the following parameters in the `46xxsettings.txt` file:

Parameter	Default value	Description
ENABLE_CALENDAR	0	Specifies whether the Calendar tab is available on Avaya Vantage™ Connect. You can assign one of the following values: • 0: To disable calendar integration with Avaya Vantage™ Connect. The Calendar tab becomes unavailable. • 1: To enable calendar integration with Avaya Vantage™ Connect. The Calendar tab becomes available. The device user can also enable or disable the Calendar tab through the Avaya Vantage™ Connect application settings.

Table continues…

Parameter	Default value	Description
EWSENABLED	0	Specifies whether EWS is enabled. Avaya Vantage™ Connect can access Microsoft Exchange Calendar information only when EWS is enabled. You can assign one of the following values: • 0: To disable EWS. • 1: To enable EWS.
EWSSERVERADDRESS	Null	Specifies the server address that can be used to connect to EWS directly. If you configure this parameter, the application tries to establish a connection to EWS directly using the server address and avoids the auto discovery process.
EWSDOMAIN	Null	Specifies the Microsoft Exchange server domain to which Avaya Vantage™ Connect must register. Avaya Vantage™ Connect uses this parameter for auto discovery of the domain if the domain is not part of the Microsoft Exchange or unified login user name.
EWSSSO	1	Specifies whether EWS uses dedicated login credentials or unified login credentials for the Microsoft Exchange server connection. You can assign one of the following values: • 0: To disable the use of unified login credentials. On the Calendar tab, you must enter the Microsoft Exchange user credentials manually to view calendar information. • 1: To enable the use of unified login credentials. If you log in to Avaya Vantage™ using unified login credentials, you do not need to log in to the Exchange Calendar service separately. • 4: To enable the use of Microsoft Modern authentication. The Calendar tab displays the Microsoft Sign in page for entering your Microsoft Exchange user account information.

Avaya Connect Expansion Module configuration

In an Avaya Aura® or IP Office environment, you can enable the use of the Avaya Connect Expansion Module application with Avaya Vantage™ Connect to extend the number of call feature buttons and line appearances.

You can install the Expansion Module application on:

- The same Avaya Vantage™ device that has Avaya Vantage™ Connect as the active telephony application.
- Another Avaya Vantage™ device with another instance of Avaya Vantage™ Connect or a different Avaya™ Client SDK application installed.

When connected with Avaya Vantage™ Connect, Expansion Module provides the feature buttons that you assign to the SIP user extension, which is used to log in to the Avaya Vantage™ device.

Feature buttons supported by Avaya Connect Expansion Module

The Avaya Connect Expansion Module application works in an Avaya Aura® or IP Office environment. The following table lists the feature buttons that are supported in each environment.

Feature buttons supported in an Avaya Aura® environment	Feature buttons supported in an IP Office environment
• Priority call • Send all calls – to voice mail • Forward all calls • Forward busy, no answer calls • Enhanced call forwarding • Exclusion • Extension to Cellular (EC500) • Extend call • Call park • Call unpark • Automatic callback • Autodial[8] • Whisper page • Group call pickup • Extended call pickup • Directed call pickup • Busy indicator • Hunt group busy position • Team Button • Bridged Line Appearance (BLA)	• Priority call • Dial paging • Dial Direct • Forward unconditional • Forward on busy • Forward on no answer • Forward number • Forward busy number • Cancel all forwarding • Hunt group enable • Twinning (EC500) • Voicemail enable • Ringback when free • Logout • Conference – Add someone • Call record • Do Not Disturb

For information about configuring call features in an Avaya Aura® environment, see the following documents:

- *Avaya Aura® Communication Manager Feature Description and Implementation*
- *Administering Avaya Aura® Communication Manager*

[8] Autodial is supported only when you configure the feature button in System Manager with a phone number. Otherwise, the Expansion Module application does not display the feature button.

After you set up features in your environment, you can assign these features to SIP users. For information about assigning feature buttons to SIP users in an Avaya Aura® environment, see *Administering Avaya Aura® System Manager*

For information about configuring call features and assigning feature buttons to SIP users in an IP Office environment, see the following documents:

- If you are using IP Office Manager, see *Administering Avaya IP Office™ Platform with Manager*
- If you are using IP Office Web Manager, see *Administering Avaya IP Office™ Platform with Web Manager*

Expansion Module configuration checklist

This checklist summarizes the setup and configuration requirements for using Expansion Module with Avaya Vantage™ Connect.

No.	Task	Notes	✔
1	In your environment, set up call features that you want to use through Expansion Module.	In an Avaya Aura® environment, ensure that call features are set up in Communication Manager. For more information, see the respective chapter on each call feature in the following documents: • *Avaya Aura® Communication Manager Feature Description and Implementation* • *Administering Avaya Aura® Communication Manager* In an IP Office environment, configure call features through IP Office Web Manager or IP Office Manager. For more information, see the following documents: • If you are using IP Office Manager, see *Administering Avaya IP Office™ Platform with Manager* • If you are using IP Office Web Manager, see *Administering Avaya IP Office™ Platform with Web Manager*	
2	Assign feature buttons to SIP users.	In an Avaya Aura® environment, configure SIP user details through the System Manager web console to assign feature buttons to the appropriate user extensions. For more information, see Adding a feature button to the SIP endpoint through System Manager on page 157. In an IP Office environment, configure the SIP user details through IP Office Web Manager or IP Office Manager to assign feature buttons to the appropriate user extensions. For more information, see Adding a feature button to the	

Table continues…

No.	Task	Notes	✔
		SIP endpoint through IP Office Web Manager on page 159.	
3	Push the Avaya Connect Expansion Module application to the designated Avaya Vantage™ devices.	Use the PUSH_APPLICATION parameter to install the Expansion Module application on the device. You can install Expansion Module on the same device as Avaya Vantage™ Connect or on a separate device with another Avaya™ Client SDK application. To install Expansion Module on a separate device, you can define a separate user group in the `46xxsettings.txt` file. Ensure that the devices with Avaya Vantage™ Connect and Expansion Module are on the same subnet. For more information about pushing applications to the device, see Pushing applications onto the Avaya Vantage device on page 128. Fore more information about user group configuration, see User group configuration in the settings file on page 114.	
4	Enable the Expansion Module service on Avaya Vantage™ Connect.	Use the BUTTON_MODULE_ENABLE parameter to enable the Expansion Module service on Avaya Vantage™ Connect. This parameter also defines whether the Avaya Vantage™ Connect user can enable or disable the Expansion Module service through the **User Settings** menu on Avaya Vantage™ Connect. An Expansion Module application can discover, pair, and connect with Avaya Vantage™ Connect only when the Expansion Module service is enabled on Avaya Vantage™ Connect. You can assign one of the following values: • 0: The Expansion Module service is disabled on Avaya Vantage™ Connect. Avaya Vantage™ Connect does not provide an option in the **User Settings** menu to enable the service. • 1: The Expansion Module service is always enabled on Avaya Vantage™ Connect. The Avaya Vantage™ Connect user cannot disable the service through the application's **User Settings** menu. Avaya Vantage™ Connect provides additional options to enable network discovery by Expansion Module applications. • 2: By default, the Expansion Module service is disabled on Avaya Vantage™ Connect. The Avaya Vantage™ Connect user can enable or disable the service through the application's **User Settings** menu. Avaya Vantage™ Connect provides additional options to enable network discovery by Expansion Module applications.	

Adding a feature button to the SIP endpoint through System Manager

About this task

In an Avaya Aura® environment, Communication Manager provides advanced call features. After you configure call features in Communication Manager, you can use this procedure to assign call feature buttons to SIP user extensions through the System Manager web console.

For more information about assigning feature buttons to a SIP user, see *Administering Avaya Aura® System Manager*.

Before you begin

Ensure that:

- A SIP user profile is created with the correct template for Avaya Vantage™. For more information, see User configuration to support Avaya IX Workplace Client and Avaya Vantage Connect as the SIP telephony application on page 23.
- Call features you want to assign to a SIP user are set up in Communication Manager. For more information about configuring call features, see the respective chapters on each call feature in the following documents:
  - *Avaya Aura® Communication Manager Feature Description and Implementation*
  - *Administering Avaya Aura® Communication Manager*

Procedure

1. On the System Manager web console, go to **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints**, and search for the extension to which you want to add feature buttons.
2. Select the user extension and click **Edit**.
3. On the Button Assignment tab, click **Feature Buttons** or **Button Module**.
4. **(Optional)** In Endpoint Configurations, in the **Button Label** field, type a name for the button.

   For example, type `Call pick up`.

   If you keep the field empty, a default label for the selected feature button is used.
5. In Button Configurations, in the **Button Feature** field, click the feature button that you want to add.

   For example, click **call–pkup** to add the Call Pickup feature button.
6. **(Optional)** If required, enter the appropriate values in the **Argument-<*n*>** fields.

   For example:

   For Team Button, you must enter the extension of the monitored station and define the ring behavior. Type `r` if you want the extension to ring or `n` for no ringing.

For the Call Pickup feature, in the **Rg** field, type `continuous` for the endpoint to ring continuously for a call pickup alert.

7. Click **Commit**.

Example: Administering call pickup

About this task

Before you assign a feature button to a SIP user extension, you must set up the call feature on Communication Manager. For the call pickup feature, following are the high-level configuration steps that you need to complete if you want members of a pickup group to receive audio and visual alerts on their device when a member of the group receives a call.

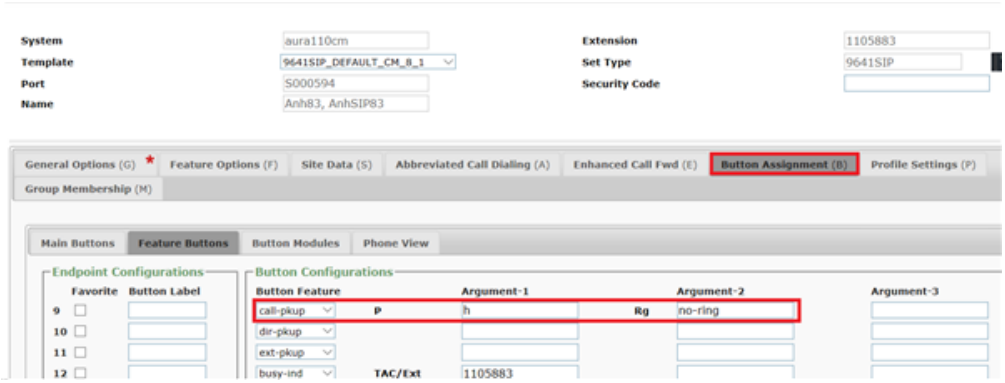
Procedure

1. On Communication Manager, enable Call Pickup Alerting and Enhanced Call Pickup Alerting:
   a. Type `change system-parameters features`.
   b. On page 19 of the Feature-Related System Parameters screen, set **Call Pickup Alerting** and **Enhanced Call Pickup Alerting** fields to `y`.
   c. Type `change cor n`, where n is the COR number assigned to the extension in the pickup group.
   d. On page 2 of the Class of Restriction screen, set the **Block Enhanced Call Pickup Alerting** field to `n`.
   e. Save the changes.

   For more information, see the “Setting up Call Pickup” section in *Avaya Aura® Communication Manager Feature Description and Implementation*.
2. Add a pickup group and assign users to the pickup group.

   For more information, see the “Adding pickup groups” section in *Avaya Aura® Communication Manager Feature Description and Implementation*.
3. On the System Manager web console, assign a **Call Pickup** button to each extension in the pickup group.
   a. Navigate to **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints**, and search for the extension.
   b. Select the user extension and click **Edit**.
   c. On the Button Assignment tab, click **Feature Buttons**.
   d. In Button Configurations, in the **Button Feature** field, click **call–pkup**.
   e. In the **Rg** field, indicate how you want the extension to ring for call pickup alerts.

      Currently, Avaya Vantage™ Connect only supports `continuous` ringing.



4. Click **Commit**.

Adding a feature button to the SIP endpoint through IP Office Web Manager

About this task

In an IP Office environment, you can add feature buttons for a SIP user extension through IP Office Manager or IP Office Web Manager. This procedure describes how to add feature buttons using IP Office Web Manager. For information about using IP Office Manager, see *Administering Avaya IP Office™ Platform with Manager*.

For more information about using IP Office Web Manager, see *Administering Avaya IP Office™ Platform with Web Manager*.

Important:

In IP Office, you can configure additional feature buttons that are supported on other Avaya phones, such as Avaya J100 Series IP Phones, but not on the Avaya Connect Expansion Module application. Expansion Module verifies the configured feature buttons and only displays the buttons that it supports.

Procedure

1. On IP Office Web Manager, navigate to **Call Management** > **Users**, and search for the user extension to which you want to add feature buttons.
2. Click ✎ next to the user.
3. Click **Button Programming**.
4. To add or edit features, click ✎.
5. In **Action**, select the feature button that you want to add.
6. **(Optional)** In the **Label** field, type a custom label for the feature button.

   If you leave this field empty, IP Office uses a default label.

If you selected a local language from **User** > **Locale**, default labels are displayed in that language. However, custom labels are not translated. If you enter a custom label in English, the feature button uses that English label regardless of what the locale is set to.

7. Click **OK**.
8. Click **Update**.

Chapter 13: Maintenance

Restoring factory settings from the Settings menu

About this task

Use this procedure to remove all user information stored on the device and to restore original manufacturer settings. This procedure describes how to perform a factory reset from the **Settings** menu on the device. You can also perform a factory reset from the boot recovery menus.

Resetting a device removes the following information from the device:

- All administered values
- User-specified data, including information about all accounts
- Device settings
- Application data and settings that were not loaded as part of the device firmware
- Wi-Fi network configuration

To be able to recover settings or data after a factory reset, you must back them up using a personal third-party account, such as Google™ account.

Before you begin

You must have the administrator password that is set through ADMIN_PASSWORD or PROCPSWD.

In an Avaya Aura® environment, if the complex password is configured in System Manager, use that password as the administrator password. If it is not available, use ADMIN_PASSWORD or PROCPSWD.

In an IP Office environment, set ADMIN_PASSWORD using the `SET_ADMINPSWD=x` NUSN, where `x` is the password that is added to the autogenerated `46xxsettings.txt` file. For example:

```
SET_ADMINPSWD=Avaya@1234
```

Procedure

1. Tap **Settings**.
2. In the upper-right corner of the screen, tap **Menu** > **Admin login**, and enter the administrator password.
3. Tap **System** > **Reset options** > **Factory data reset**.
4. Tap **Reset device**.

5. Tap **Erase everything**.

   The device restarts. The process takes approximately 20 minutes to complete.

Related links

Firmware is corrupted on page 184

Clearing user data stored in PPM

About this task

In an Avaya Aura® environment, Avaya Vantage™ uses PPM as the backup server to back up and restore user preferences or settings for a device related to the user account. Parameter settings stored in PPM takes precedence over the same parameter settings retrieved from the `46xxsettings.txt` file. If you want the Avaya Vantage™ device to use settings retrieved from the `46xxsettings.txt` file instead of the values stored in PPM, you can clear such user settings from PPM through the device **Settings** menu.

This procedure is not applicable in an IP Office environment.

Before you begin

You must have the administrator password that is set through ADMIN_PASSWORD or PROCPSWD.

In an Avaya Aura® environment, if the complex password is configured in System Manager, use that password as the administrator password. If it is not available, use ADMIN_PASSWORD or PROCPSWD.

Procedure

1. Tap **Settings**.
2. In the upper-right corner of the screen, tap **Menu** > **Admin login**, and enter the administrator password.
3. Tap **System** > **Reset options**.
4. Tap **Clear user data in PPM**.
5. Tap **Yes** to confirm.

Rebooting Avaya Vantage™ from the Settings menu

About this task

Use this procedure to restart Avaya Vantage™ manually. You can also reboot Avaya Vantage™ to initiate an upgrade.

Procedure

1. Go to the **Settings** menu.
2. Tap **System** > **Reset options**.
3. Tap **Reboot** and then tap **Yes** to confirm.

   If the file server contains a new version of software, Avaya Vantage™ downloads and installs updates according to the configured upgrade policy.

Failover and survivability

If the control server that is currently active fails, the exact behavior of a communication application is determined by the application's internal policies. The exact list of operations that can be performed during failover might be different for each application.

Debugging and monitoring options

Avaya Vantage™ enables you to generate debug and audio debug reports that support personnel can use to diagnose audio and video issues on the device. The debug report contains various detailed logs. You can also generate a separate audio report that contains only audio logs. You can enable SSH remote access on the device for Avaya support personnel to access the device for remote troubleshooting.

When you are using the Avaya IX™ Workplace Client as the active telephony application on Avaya Vantage™, you can also allow the client to collect detailed diagnostic logs and quality-related data. From the Avaya IX™ Workplace Client settings, navigate to the Support tab and turn on **Enable Diagnostics**. Additionally, you can view the audio and video statistics of an ongoing conference call by pressing and holding the call timer on Avaya IX™ Workplace Client. For more information about collecting diagnostics and quality statistics, see:

- "Support, alerts, and log files" in *Using Avaya IX™ Workplace Client for Android, iOS, Mac, and Windows*.
- "Network considerations and diagnostics" in *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac, and Windows*.

Enabling verbose logging

About this task

Use this procedure to configure syslog and local logging, and to set the scope of log messages and the events to be included in log messages.

Before you begin

You must have the administrator password that is set through ADMIN_PASSWORD or PROCPSWD.

In an Avaya Aura® environment, if the complex password is configured in System Manager, use that password as the administrator password. If it is not available, use ADMIN_PASSWORD or PROCPSWD.

Procedure

1. On the Home screen, tap **Applications**.
2. Tap **Settings**.
3. In the upper-right corner of the screen, tap **Menu** > **Admin login**, and enter the administrator password.
4. Tap **Debugging options**.
5. Tap **Log**.
6. Tap **Log Categories** and select the log categories to be included in log messages.
7. To configure syslog for remote logging, do the following:
   a. On the Log screen, tap **Remote Logging**.
   b. Move the **Remote Logging** slider to the right to enable remote logging.
   c. Tap **Remote Log Level**, and select the severity level of syslog messages.

      The device sends a syslog message if a severity level of an event is equal or less than the selected log level. The default settings is Error.
   d. Tap **Remote Log Server**, and enter the address of the server where you want syslog messages to be stored.
8. To configure local logging, do the following:
   a. On the Log screen, tap **Local logging**.
   b. Move the **Local Logging** slider to the right to enable local logging.
   c. Tap **Local Log Level**, and select the severity level of events to be included in log messages.

      The device stores a log message if the severity level of an event is equal or less than the selected log level. The default setting is Warnings.
   d. Tap **Clear Local Log Files** to delete local log files and core dump files.

Generating a debug report

About this task

Use this procedure to generate a debug report that captures detailed event and audio logs for use by support personnel. The debug option is also available when you are logged out of the device.

You can save the report in the internal flash memory of Avaya Vantage™, on a USB mass storage device, or on an HTTP or HTTPS server. When you generate a debug report, Avaya Vantage™ overwrites any existing report, if applicable. The report remains available in the internal flash memory for up to 14 days.

Record the encryption password carefully because you cannot decrypt the report without the password.

Before you begin

To save the report on a USB mass storage device, connect it to the Avaya Vantage™ device.

Procedure

1. Tap **Settings**.
2. Tap **Debugging options** > **Generate debug report**.
3. **(Optional)** On the Debug report page, complete the following information as required:
   - **Select date that the problem was observed**
   - **Select time that the problem was observed**
   - **Select Problem**
   - **Problem Description**
4. Enter the password for encryption and decryption of the report.

   If the DEBUG_REPORT_PASSWORD parameter is configured, the password is populated automatically based on the parameter value. The password is masked in the field. You cannot modify the password that comes from the DEBUG_REPORT_PASSWORD parameter.
5. Select one of the following destinations to store the report:
   - **Internal flash memory**
   - **HTTP/S file server**
   - **USB flash drive**

     The **USB flash drive** option is available only when a USB mass storage device is already connected to Avaya Vantage™.

   On K155, you must scroll down to view and select an option.

   Tip:

   To copy and share a report easily from K155, Avaya recommends that you choose the **HTTP/S file server** or **USB flash drive** option to store the report. If you store the report in the internal flash memory on K155, you need to follow a different procedure to retrieve the report from the internal memory.
6. **(Optional)** If you select the **HTTP/S file server** option, enter the HTTP or HTTPS server address and path, as well as the user name and password if server authentication is required.

   You can enter an IPv4 or IPv6 address, or an FQDN.

If the BRURI parameter is configured, the HTTP/S server details are populated automatically in the respective fields based on the BRURI value. You cannot change these values.

If the BRURI parameter is not configured, the HTTP/S server detail entries are saved for the next debug or audio reports. You can modify these details.

7. Tap **Generate**.

   Avaya Vantage™ generates a debug report, `debugreport.tar.gz.enc`, and stores it in the internal flash memory at `/mnt/sdcard/AvayaVantageLogs`. If you select the USB flash drive or HTTP/S option, a copy of the report is saved in the selected destination.

8. **(Optional)** On K165 and K175, to share the report, click <.

   You can share the report through most email systems and Google Drive.

   The success of the sharing operation depends on the file size and the selected option. For example, while most email systems support an attachment that is up to 20 MB only, Google Drive can support up to 10 GB.

   The < icon is not available if you are logged out of the device.

Related links

Copying debug report from internal flash memory on page 168

Generating an audio report

About this task

Use this procedure to generate a separate audio debug report instead of a complete debug report. The audio debugging option is also available when you are logged out of the device.

You can save the report in the internal flash memory of Avaya Vantage™, on a USB mass storage device, or on an HTTP or HTTPS server. When you generate an audio report, Avaya Vantage™ overwrites any existing report, if applicable. The report remains available in the internal flash memory for up to 14 days.

Ensure that you record the encryption password carefully because you cannot decrypt the report without the password.

Before you begin

- To enable audio debug recording, ensure that ENABLE_RECORDING is set to `1`. You can set this parameter in the settings file or through Avaya Aura® Device Services for Avaya Aura® deployments.
- To save the report on a USB mass storage device, connect it to the Avaya Vantage™ device.

Procedure

1. Tap **Settings**.
2. Tap **Debugging options** > **Generate audio report**.

3. **(Optional)** On the Audio report page, complete the following information as required:
   - **Select date that the problem was observed**
   - **Select time that the problem was observed**
   - **Select Problem**
   - **Problem Description**
4. Enter the password for encryption and decryption of the report.

   If the DEBUG_REPORT_PASSWORD parameter is configured, the password is populated automatically based on the parameter value. The password is masked in the field. You cannot modify the password that comes from the DEBUG_REPORT_PASSWORD parameter.
5. Select one of the following destinations to store the report:
   - **Internal flash memory**
   - **HTTP/S file server**
   - **USB flash drive**

     The **USB flash drive** option is available only when a USB mass storage device is already connected to Avaya Vantage™.

   On K155, you must scroll down to view and select an option.

   Tip:

   To copy and share a report easily from K155, Avaya recommends that you choose the **HTTP/S file server** or **USB flash drive** option to store the report. If you store the report in the internal flash memory on K155, you need to follow a different procedure to retrieve the report from the internal memory.
6. **(Optional)** If you select the **HTTP/S file server** option, enter the HTTP or HTTPS server address and path, as well as the user name and password if server authentication is required.

   You can enter an IPv4 or IPv6 address, or an FQDN.

   If the BRURI parameter is configured, the HTTP/S server details are populated automatically in the respective fields based on the BRURI value. You cannot change these values.

   If the BRURI parameter is not configured, the HTTP/S server detail entries are saved for the next debug or audio reports. You can modify these details.
7. Tap **Generate**.

   Avaya Vantage™ generates an audio report, `media_report.tar.gz.enc`, and stores it in the internal flash memory at `/mnt/sdcard/AvayaVantageLogs`. If you select the USB flash drive or HTTP/S option, a copy of the report is saved in the selected destination.
8. **(Optional)** On K165 and K175, to share the report, click <.

   You can share the report through most email systems and Google Drive.

The success of the sharing operation depends on the file size and the selected option. For example, while most email systems support an attachment that is up to 20 MB only, Google Drive can support up to 10 GB.

The icon is not available if you are logged out of the device.

Related links

Copying debug report from internal flash memory on page 168

Copying debug report from internal flash memory

About this task

Use this procedure to copy log reports from the internal flash memory of Avaya Vantage™ to a USB flash drive. This procedure is useful to retrieve a debug report from the internal flash memory of a K155 device, which does not support the Android share option.

Before you begin

Connect the USB flash drive to the Avaya Vantage™ device.

Procedure

1. Tap **Settings**.
2. Tap **Storage** > **Files** > **AvayaVantageLogs**.
3. Long press the debug archive file to select it.
4. In the upper-right corner of the screen, tap **More Menu** > **Move to**.
5. On the new page, tap ≡ and then choose **USB DRIVE**.
6. Tap **MOVE**.

Opening a debug or audio report

About this task

Use this procedure to decrypt a debug or audio report. To review log data, you must decrypt the reports.

Before you begin

Ensure that the OpenSSL library is installed on the system from where you want to decrypt the reports.

- On a Linux system, OpenSSL comes with the operating system distribution package. Else, download the latest OpenSSL package and install.
- On a Windows system, download Windows binaries of OpenSSL.

Procedure

1. Copy the report to a folder on your computer.

2. Open the command line interface and navigate to the folder where you copied the report.
3. Do one of the following to decrypt the debug report:
   - On a Linux system, run the following command:

     ```
     openssl aes-256-ctr -md sha256 -d -salt -k <password> -in
     debugreport.tar.gz.enc -out <decrypted_file>.tar.gz
     ```

   - On a Windows system, navigate to the folder where the `openssl.exe` file is extracted, and run the following command:

     ```
     openssl.exe aes-256-ctr -md sha256 -d -salt -k <password> -in
     debugreport.tar.gz.enc -out <decrypted_file>.tar.gz
     ```

   Replace *<password>* with the password that you provided when generating the report.

   Replace *<decrypted_file>* with an archive file name where the decrypted reports are to be saved.
4. Do one of the following to decrypt the audio report:
   - On a Linux system, run the following command:

     ```
     openssl aes-256-ctr -md sha256 -d -salt -k <password> -in
     media_report.tar.gz.enc -out <decrypted_file>.tar.gz
     ```

   - On a Windows system, navigate to the folder where the `openssl.exe` file is extracted, and run the following command:

     ```
     openssl.exe aes-256-ctr -md sha256 -d -salt -k <password> -in
     media_report.tar.gz.enc -out <decrypted_file>.tar.gz
     ```

   Replace *<password>* with the password that you provided when generating the report.

   Replace *<decrypted_file>* with an archive file name where the decrypted reports are to be saved.
5. To extract the decrypted archive file, do one of the following:
   - On Windows-based computers, use any program that can extract zip archives.
   - On Linux systems, run the following command:

     ```
     tar -zxvf <decrypted_file>.tar.gz
     ```

Configuring the SSH server settings

About this task

Use this procedure to enable challenge-response authentication on SSH for Avaya support personnel or personal access only.

Before you begin

You must have the administrator password that is set through ADMIN_PASSWORD or PROCPSWD.

In an Avaya Aura® environment, if the complex password is configured in System Manager, use that password as the administrator password. If it is not available, use ADMIN_PASSWORD or PROCPSWD.

Procedure

1. Tap **Settings**.
2. In the upper-right corner of the screen, tap **Menu** > **Admin login**, and enter the administrator password.
3. Tap **Debugging options** > **SSH server settings**.
4. **(Optional)** To enable SSH remote access to the device, enable **SSH server mode**.
5. **(Optional)** To enable sroot access to the device, enable **SSH server root mode**.

Enabling port mirroring

About this task

Use this procedure to copy the Ethernet packets that are transmitted or received on the network to the secondary Ethernet port.

This functionality is only available if you have an embedded Ethernet switch on Avaya Vantage™.

Before you begin

You must have the administrator password that is set through ADMIN_PASSWORD or PROCPSWD.

In an Avaya Aura® environment, if the complex password is configured in System Manager, use that password as the administrator password. If it is not available, use ADMIN_PASSWORD or PROCPSWD.

Procedure

1. Tap **Settings**.
2. In the upper-right corner of the screen, tap **Menu** > **Admin login**, and enter the administrator password.
3. Tap **Debugging options** > **Port mirroring**.
4. Select the **Port mirroring** check box.

Pinging a device on the network

About this task

Use this procedure to ensure that Avaya Vantage™ can reach a particular IP address or a host on the network.

This option is also available when you are logged out of the device.

Procedure

1. Tap **Settings**.
2. Tap **Debugging options** > **Host to ping**.
3. Enter the IP address or host name of the device.

   You can enter an IPv4 or IPv6 address, or an FQDN.
4. Tap **OK**.

   If Avaya Vantage™ can resolve the IP address, it displays the ping statistics that include the number of packets transmitted and received, packet loss percentage, and time taken.

SLA Mon™ for diagnostics

SLA Mon™ is a patented Avaya technology that facilitates advanced diagnostics. The SLA Mon™ agent works with the Avaya Diagnostic Server. On Avaya Vantage™, the SLA Mon™ agent can execute the following advanced diagnostic functions:

- Perform network QoS tests and monitoring. This involves sending RTP and trace route messages between SLA Mon™ agents.
- Capture packets with or without RTP headers for audio and video calls.

The device user receives a notification when you initiate a packet capture.

Enabling SLA Mon™ agent functionality

To use SLA Mon™ agent functionality, ensure the following:

- The SLMSTAT parameter in the settings file is set to 1. By default, this parameter is set to 0 (Disabled).
- The SLMSRVR parameter is set to the IP address of the SLA Mon™ server.

You must configure additional parameters to define how the SLA Mon™ features will work. For detailed information about SLA Mon™ parameters, see SLA Mon agent settings on page 306.

Certificate usage

You must download the SLA Mon™ server identity root CA certificate to the device through the TRUSTCERTS parameter for the server authentication. There is no embedded Avaya SIP root CA certificate built in to Avaya Vantage™ or the SLA Mon™ agent. After downloading trusted certificates based on TRUSTCERTS, Avaya Vantage™ uses these certificates to authenticate the server certificate. You can use a certificate issued by a Certificate Authority (CA) or an in-house CA, or use a self-signed certificate. Intermediate certificates are also supported.

If a subjectAltName extension of type DNSName is present, that must be used as the identity certificate. Otherwise, the Common Name in the Subject field of the certificate is used.

In some cases, the URI is specified as an IP address rather than a host name. In this case, the subjectAltName IP address must be present in the certificate and must exactly match the IP address in the URI.

Chapter 14: Device upgrade

You must upgrade the Avaya Vantage™ firmware to keep the device up-to-date, gain access to new features, and enhance stability and security.

Avaya Vantage™ downloads upgrade images and configuration files from an HTTP or HTTPS file server.

Avaya Vantage™ firmware upgrade options

You can perform a device firmware upgrade in the following ways:

- Automatic: Configure the device to poll periodically for a newer version of the software in the file server and automatically download the upgraded software.

  In an IP Office environment, the IP Office system uses the push method for software upgrades. Therefore, you must disable the automatic poll mechanism by setting the UPGRADE_POLICY parameter to 0.

- Manual: Upgrade the device manually without the device waiting for a polling interval by:
  - Using the **Update now** option in the **Settings** > **System** > **About Avaya Vantage** > **Software information** menu on the device. With this option, the device immediately downloads and installs the software if an updated software version is available.
  - Rebooting the device from the **Settings** > **System** > **Reset options** menu on the device, System Manager, IP Office System Status Application, or IP Office System Monitor. If an updated version of software is available, then the device upgrades immediately after the reboot or later according to the upgrade policy configured for the device.

Firmware upgrades in Device Enrollment Services

You can view supported device versions and enable automatic firmware upgrades in Device Enrollment Services. In the Device Enrollment Services web interface, navigate to **Device Family** to view the latest supported firmware version and the minimum version required for device enrollment. For information about enabling automatic firmware upgrades, see “Enabling or disabling device firmware upgrades” in *Using Avaya Device Enrollment Services to Manage Endpoints*.

Device upgrade process

Avaya Vantage™ upgrade images consist of packages. During the upgrade process, Avaya Vantage™ downloads and installs only new or changed packages from the upgrade image.

To perform an upgrade, Avaya Vantage™ does the following:

1. Receives the file server address from DHCP, LLDP, Device Enrollment Services, or the device interface.
2. Connects to the file server and searches for the `K1xxSupgrade.txt` file.

   If IP Office is the file server, it auto-generates an appropriate file unless one has been uploaded to its file storage.
3. Compares its software version with the version specified in the `K1xxSupgrade.txt` file.
4. If a newer version of a software distribution package is available, downloads the required package.
5. Applies the new software.
6. Locates and downloads the `46xxsettings.txt` settings file that is specified in the `K1xxSupgrade.txt` file.

   You must ensure that the `46xxsettings.txt` file is available on the file server. Otherwise Avaya Vantage™ does not apply the software updates.

   If IP Office is the file server, it auto-generates an appropriate file and adjusts various settings in that auto-generated file to match the settings in the IP Office system configuration.

Firmware upgrade prerequisites

Before upgrading the device firmware, you must perform the following actions:

- Provide a path to the file server in the FILE_SERVER_URL parameter. The device can receive the file server address from DHCP, LLDP, Device Enrollment Services, or the device interface.

  Note:

  If FILE_SERVER_URL is not defined, Avaya Vantage™ uses HTTPSRVR, HTTPPORT, and HTTPDIR for an HTTP file server, or TLSSRVR, TLSPORT, and TLSSIR for an HTTPS file server.
- Ensure that the upgrade-related parameters, such as UPGRADE_POLICY and UPGRADE_POLLING_PERIOD, that control the upgrade policy are set correctly in the `46xxsettings.txt` file according to your requirement.
- Save the updated `46xxsettings.txt` settings file on the file server.

  If you change the parameter configuration for the upgrade policy, Avaya Vantage™ implements these changes after a reboot or the next polling. Therefore, reboot the device or wait for the next polling period to occur before downloading the latest firmware distribution package to the file server.
- Download the newest firmware distribution package on the file server.

Related links

File server setup on page 36
Setting up a file server on page 38
Downloading device firmware on page 39
Device configuration using a 46xxsettings.txt settings file on page 111

Parameters for defining upgrade policy

To define the upgrade policy for Avaya Vantage™ devices, you can set the following parameters:

Parameter	Default value	Description
UPGRADE_POLLING_PERIOD	60	Specifies the interval between two consecutive attempts of polling the upgrade files and the settings files. The polling interval is measured in minutes. Assign one of the following values: • 0: Polling is disabled. • 5 to 10080: Polling is enabled. The minimum polling interval you can define is 5 minutes. The parameter value range supported by Avaya Vantage™ is 0, 5-10080. If you define a value from 1 to 4, Avaya Vantage™ considers it as invalid and takes the default value of 60 minutes. In each polling, the upgrade files and the settings files are downloaded if modified. If any change is identified to the settings file, then the device applies the new settings. The device checks whether a newer version of the firmware is available on the file server. If a newer version is detected, then it is downloaded and installed according to the upgrade rules defined by the parameters UPGRADE_POLICY, UPGRADE_DLOAD_START, UPGRADE_DLOAD_END, UPGRADE_INSTALL_DATE_TIME, DLOAD_RND_AFTER_RESET, and DLOAD_RND. If the UPGRADE_POLICY value is 0, then UPGRADE_POLLING_PERIOD is ignored. The upgrade and settings files are downloaded only after a reboot. For upgrades to take place immediately after a polling, you must set UPGRADE_POLICY to 2.

Table continues…

Parameter	Default value	Description
UPGRADE_POLICY	0	Specifies the upgrade policy. Assign one of the following values: • 0: Avaya Vantage™ downloads and installs the firmware files after a reboot only. The device does not automatically poll the server for upgrade and configuration files at intervals. For IP Office deployments, use this value. • 1: Avaya Vantage™ downloads and installs the firmware files according to upgrade policy rules and management application settings. Avaya Vantage™ does not perform the upgrade after a reboot. • 2: Avaya Vantage™ downloads and installs the firmware files after any reboot and according to upgrade policy rules and management application settings. **Note:** If you want to enforce an immediate upgrade at a device reboot instead of waiting for a scheduled upgrade, set the UPGRADE_POLICY value to 2.
UPGRADE_DLOAD_START	00	Specifies a time when Avaya Vantage™ starts trying to download new upgrade image files. The value of parameter is a string in the `[Ddd]hh` format, where: • `[Ddd]` is a day of the week. The valid values are `Sun`, `Mon`, `Tue`, `Wed`, `Thu`, `Fri`, or `Sat`. This component is optional. If the component is omitted, Avaya Vantage™performs polling every day. • `hh` is one or two numeric digits representing the hour of the day. The range is from 0 to 23. If the value of UPGRADE_DLOAD_START is equal to the value of UPGRADE_DLOAD_END, then no polling period is specified and Avaya Vantage™ can download upgrade files at any time. UPGRADE_DLOAD_START and UPGRADE_DLOAD_END are ignored if UPGRADE_POLICY is set to 0. These parameters are applicable only when UPGRADE_INSTALL_DATE_TIME is configured to a *future* date.
UPGRADE_DLOAD_END	00	Specifies a time when Avaya Vantage™ stops trying to download new upgrade image files. Even after the specific time is up, any ongoing file downloads are taken to completion. However, new file downloads are scheduled for the next download timeframe. The parameter value is in the format similar to UPGRADE_DLOAD_START.

Table continues…

Parameter	Default value	Description
UPGRADE_INSTALL_DATE_TIME	1970-01-01T00:00	Specifies the date and time when Avaya Vantage™ starts to install the downloaded upgrade files. The value of the parameter uses the `YYYY-MM-DDThh:mm` format, where: • `YYYY` is four numeric digits representing the year • `MM` is two numeric digits representing the month. • `dd` is two numeric digits representing the day of the month. • `T` is the time separator. • `hh` is two numeric digits representing a hour of the day. The range is from 0 to 23. • `mm` is two numeric digits representing minutes of the hour. The range is from 0 to 59. If the default value is used or the value is set to a past date and UPGRADE_POLICY is set to 2, Avaya Vantage™ installs upgrade files immediately after downloading irrespective of other parameter definitions.
DLOAD_RND_AFTER_RESET	0	Specifies the maximum length of the interval Avaya Vantage™ waits after reboot before attempting to download the upgrade files. The interval is measured in seconds. Assign one of the following values: • 0: The interval is not specified. Avaya Vantage™ starts the download immediately after reboot. • 1 – 32767: After reboot, Avaya Vantage™ delays the download. The exact delay interval is determined as a random number in a range between 0 and the DLOAD_RND_AFTER_RESET value. Avaya recommends that you configure randomized download time in an environment where multiple devices access the file server at the same time.
DLOAD_RND	3600	Specifies the maximum length of an interval between two consecutive attempts of background downloading. The interval is measured in seconds. Assign one of the following values: • 0: The interval is not specified. Avaya Vantage™ performs background download attempts without delay. • 1 – 32767: Avaya Vantage™ inserts a delay between two background download attempts. The exact delay interval is determined as a random number in a range between 0 and the DLOAD_RND value.

Automatic upgrades

You can configure the settings file to allow Avaya Vantage™ to periodically check for a newer version of software on the file server. If the file server contains new software, Avaya Vantage™ automatically downloads and installs upgrade files. Avaya Vantage™ downloads upgrade files in the background so the download does not affect the user experience.

Automatic upgrades do not interrupt active calls. Avaya Vantage™ starts the upgrade after all calls are completed.

You can specify the following upgrade policies in the settings file:

- Schedule the download for a specific time and day of the week.
- Schedule installation for a specific date and time.
- Set the polling interval for a new image file.

For Avaya Vantage™ to automatically download and install upgrade files, set the UPGRADE_POLICY parameter value to 1 or 2.

Related links

Parameters for defining upgrade policy on page 174

Scenario: Performing a scheduled upgrade

About this task

This scenario describes how to perform a scheduled upgrade for multiple Avaya Vantage™ devices together on January 25, 2019.

Procedure

1. Ensure that the devices to be upgraded point to the correct file server address.
2. In the settings file, set the following parameters for the scheduled upgrade:

```
SET UPGRADE_DLOAD_START 22
SET UPGRADE_DLOAD_END 23
SET UPGRADE_POLICY 1
SET UPGRADE_INSTALL_DATE_TIME 2019-01-25T22:00
```

Important:

Defining UPGRADE_INSTALL_DATE_TIME correctly is very important. If the value is set to a past date or left at the default setting, the installation date is considered to be missed and Avaya Vantage™ starts downloading and installing upgrade files immediately irrespective of other parameter definitions.

3. Save the updated file on the file server.
4. Wait for the next polling period to occur so that the device downloads the settings file and applies the new upgrade schedule.

Avaya Vantage™ downloads the settings file and applies the configuration based on the polling interval that you define in UPGRADE_POLLING_PERIOD. Do not download the firmware distribution package to the file server before the polling occurs. Otherwise, the device will download the package and start upgrading according to the earlier upgrade rules instead of the new upgrade schedule.

5. Download the latest firmware distribution package to the file server.

Result

Every night from 10 PM to 11 PM until January 25, 2019, Avaya Vantage™ tries to download the new image files from the file server. At 10 PM on 2019-01-25, all devices pointing to the file server are upgraded together. The UPGRADE_POLICY value of 1 ensures that the devices do not upgrade during a reboot before the scheduled date and time.

If you want devices to upgrade at a reboot as well as at the scheduled time, set the UPGRADE_POLICY value to 2.

Upgrading Avaya Vantage™ using the Update option

About this task

Use this procedure to manually check for upgrade files and to download and install upgrade files immediately if updated software is available.

Procedure

1. Go to the **Settings** menu of the device.
2. Tap **System** > **About Avaya Vantage** > **Software information**.
3. Tap **Update now**.

   If the file server contains new software, Avaya Vantage™ starts the upgrade. If Avaya Vantage™ has the latest software, the `Your phone is up to date` message is displayed on the screen.

Upgrading Avaya Vantage™ using System Manager

About this task

Use this procedure to perform a bulk upgrade of Avaya Vantage™ in the Avaya Aura® environment.

The actual procedure might differ depending on the System Manager version you are using. For more information, see *Administering Avaya Aura® System Manager*.

Procedure

1. Log in to System Manager.

2. In the System Manager interface, provide the range of Avaya Vantage™ IP addresses that require an upgrade.
3. Click **Reboot**.

   After reboot, Avaya Vantage™ downloads the upgrade file from the file server. Avaya Vantage™ compares the current version of the software with the version specified in the upgrade file. If the file server contains the newer version of software, Avaya Vantage™ performs the upgrade.

Upgrading Avaya Vantage™ using IP Office

About this task

Use this procedure to perform an upgrade of Avaya Vantage™ in the IP Office environment.

Procedure

To upgrade a specific Avaya Vantage™ device, do the following:

1. Restart the device using one of the following IP Office applications:
   - System Status Application
   - System Monitor

   For more information, see *Using Avaya IP Office™ Platform System Monitor* and *Using Avaya IP Office™ Platform System Status Application*.

   If an updated version of software is available for Avaya Vantage™, then the device upgrades immediately after the reboot.

To upgrade all Avaya Vantage™ devices, do the following:

2. Upgrade the IP Office system using the Upgrade Wizard of IP Office Manager.
3. Select the check box to restart all SIP devices in the environment after the system upgrade.

   For more information about upgrading through IP Office Manager, see *Administering Avaya IP Office™ Platform with Manager*.

   The upgrade process updates any SIP phone firmware files held on the system. If an updated version of software become available for Avaya Vantage™, then the device upgrades immediately after the reboot.

Support for two or more software versions on the same file server path

Avaya Vantage™ devices download software files from a file server according to the FILE_SERVER_URL configuration parameter. If FILE_SERVER_URL is not configured, then Avaya Vantage™ uses HTTPSRVR, HTTPPORT, HTTPDIR, TLSSRVR, TLSPORT, and TLSPDIR. The file server directory has one `K1xxSupgrade.txt` file, which points to the relevant software image for upgrade according to the APPNAME configuration parameter value.

The following is an example of the `K1xxSupgrade.txt` file:

```
## AVAYA VANTAGE DEVICE SOFTWARE UPGRADE CONFIGURATION FILE ##
##                 *** Dec 19, 2019 ***                     ##
##                                                          ##
## This file upgrades the following Telephones              ##
## to the indicated releases:                               ##
##    K165/K175     R2_2_0_1                                 ##

IF $MODEL4 SEQ K155 GOTO K155SW
IF $MODEL4 SEQ K165 GOTO K175SW
IF $MODEL4 SEQ K175 GOTO K175SW
GOTO GETSET

# K155SW
SET APPNAME K1xx_SIP-R2_2_0_1_7534.tar
GOTO GETSET

# K175SW
SET APPNAME K1xx_SIP-R2_2_0_1_7034.tar
GOTO GETSET

# GETSET
GET 46xxsettings.txt
```

If you need two different sets of Avaya Vantage™ devices to run two different software versions, use one of the following solutions:

- Use two different file servers or directories.
- Add conditional statements in the `K1xxSupgrade.txt` file, according to the GROUP value, to point to different software versions.
- Add conditional statements in the `46xxsettings.txt` file, according to the GROUP value, to point to different software versions.

You can apply the second and third solutions on any HTTP or HTTPS file server. These solutions are not applicable when you use Avaya Aura® Device Services as the file server. Avaya Aura® Device Services supports one software version for each phone family.

Two different file servers or directories

You can use two different file servers or two different directories on the same file server and copy different versions of software images to each file server or directory. In this solution, you need to duplicate the `46xxsettings.txt` file and relevant configurations in both places.

You must configure different file server paths for each set of devices. You can use the FILE_SERVER_URL parameter to specify different paths and FQDN or IP addresses. You can achieve this using the following methods:

- By connecting the two sets of devices to two different VLANs, where each VLAN is configured with different FILE_SERVER_URL value in the DHCP SSON.
- By configuring different file server addresses through each device's **Settings** menu.

You can also use HTTPSRVR, TLSSRVR, HTTPPORT, TLSPORT, HTTPDIR, or TLSDIR to differentiate between the two file servers or directories.

K1xxSupgrade.txt to point to two different software versions

Another solution is to modify the `K1xxSupgrade.txt` file to include different APPNAME values per GROUP or any other testable parameter, such as SERIALNO or MACADDR.

You can add conditional statements in the `K1xxSupgrade.txt` file, according to the GROUP parameter, value to point to different software versions.

The following is an example of using GROUP to conditionally point to different software versions. In this example, devices that are assigned to GROUP==1 will have a newer software version while the rest of the devices will have an earlier software version.

```
## AVAYA VANTAGE DEVICE SOFTWARE UPGRADE CONFIGURATION FILE ##
##                 *** Dec 19, 2019 ***                     ##

## This file upgrades the following Telephones              ##
## to the indicated releases:                               ##
##    K165/K175     R2_2_0_1                                 ##

IF $MODEL4 SEQ K155 GOTO K155SW
IF $MODEL4 SEQ K165 GOTO K175SW
IF $MODEL4 SEQ K175 GOTO K175SW
GOTO GETSET

# K155SW
IF $GROUP SEQ 1 GOTO K155NEWSW
SET APPNAME K1xx_SIP-R2_2_0_1_7534.tar
GOTO GETSET
# K155NEWSW
SET APPNAME K1xx_SIP-R2_2_0_1_7535.tar
GOTO GETSET

# K175SW
IF $GROUP SEQ 1 GOTO K175NEWSW
SET APPNAME K1xx_SIP-R2_2_0_1_7034.tar
GOTO GETSET
# K175NEWSW
SET APPNAME K1xx_SIP-R2_2_0_1_7035.tar
GOTO GETSET

# GETSET
GET 46xxsettings.txt
```

In this example, APPNAME is conditionally set according to GROUP values. You must set the APPNAME values with the actual values from the original `K1xxSupgrade.txt` file included in each software distribution package for the software versions you want to run.

For each software upgrade, a `K1xxSupgrade.txt` file is included with the software distribution package. When you download and extract a new software distribution package on the target file server directory, the new `K1xxSupgrade.txt` file included in the package overwrites the existing one in that directory. Therefore, you must modify the `K1xxSupgrade.txt` file to point to two software versions each time you apply a new software version on the target directory.

Note:

The software distribution packages include *digest* in their file names to prevent file name conflicts when you extract two software distribution packages to the same directory. Similarly, Android APK file names include the version information and therefore no file name conflict occurs when you unpack the two software distributions packages to the same directory.

46xxsettings.txt to point to two different software versions

If you do not want to modify the `K1xxSupgrade.txt` file, you can instead use the `46xxsettings.txt` file to conditionally set the APPNAME values to point to two different software versions.

You can copy the relevant part from the following configuration example to the beginning of the `46xxsettings.txt` file. In the `46xxsettings.txt` file, `# STARTCONFIG` represents the beginning of the file.

```
IF $MODEL4 SEQ K155 GOTO K155SW
IF $MODEL4 SEQ K165 GOTO K175SW
IF $MODEL4 SEQ K175 GOTO K175SW
GOTO STARTCONFIG

# K155SW
IF $GROUP SEQ 1 GOTO K155NEWSW
SET APPNAME K1xx_SIP-R2_2_0_1_7534.tar
GOTO STARTCONFIG
# K155NEWSW
SET APPNAME K1xx_SIP-R2_2_0_1_7535.tar
GOTO STARTCONFIG

# K175SW
IF $GROUP SEQ 1 GOTO K175NEWSW
SET APPNAME K1xx_SIP-R2_2_0_1_7034.tar
GOTO STARTCONFIG
# K175NEWSW
SET APPNAME K1xx_SIP-R2_2_0_1_7035.tar
GOTO STARTCONFIG

# STARTCONFIG
```

CSDK-based application upgrades

Avaya Vantage™ Connect or Avaya IX™ Workplace Client can be configured as the active CSDK-based telephony application on Avaya Vantage™. You can update the CSDK-based application on Avaya Vantage™ through the following options:

- The “Push application” method. Through the PUSH_APPLICATION parameter, you can initiate automatic installation of the latest version of the application without any intervention from the end user.
- Google Play. If a newer version of Avaya Vantage™ Connect or Avaya IX™ Workplace Client becomes available in Google Play, Avaya Vantage™ displays an upgrade notification. End users can update the application from Google Play for K165 and K175.
- Android Package Kits (APKs). These APKs of the CSDK-based applications are bundled in the Avaya Vantage™ firmware package file and pushed automatically to the Avaya Vantage™ device. If installation of applications from unknown sources is enabled, then end users can also download application APKs from other sources, such as emails or websites.

For more information about installing and updating applications on Avaya Vantage™, see the sections under Application setup on page 127.

Enabling a wireless handset upgrade

About this task

You can enable an automatic upgrade of the paired wireless handset by setting the ENABLE_CORDLESS_HANDSET_UPDATE parameter in the `46xxsettings.txt` file. By default, the handset upgrade is disabled.

If you enable the wireless handset upgrade, Avaya Vantage™ applies the update to the wireless handset automatically whenever an update is available on the file server.

Procedure

To enable the wireless handset upgrade, in the `46xxsettings.txt` file, set the ENABLE_CORDLESS_HANDSET_UPDATE parameter value to 1 as follows:

```
SET ENABLE_CORDLESS_HANDSET_UPDATE 1
```

Chapter 15: Troubleshooting

This chapter describes known troubleshooting issues that customers might encounter while performing installation, configuration, and maintenance.

Firmware is corrupted

Condition

Firmware is corrupted so you must restore firmware to its original state.

Cause

Firmware corruption can occur because of a power outage when the device is upgraded, or because of a corrupt system file or an invalid checksum file.

Solution

Use the boot recovery procedure to clear the device and restore Avaya Vantage™ to its factory settings.

Use the boot recovery menu options only when the device does not boot up properly for some reason. The boot recovery menu provides you options to delete all stored data or swap the boot banks on the device and try to bring up the Android operating system again.

1. Connect an external USB keyboard to the device.

   If the keyboard is USB Type-A, then you require a USB Type-A to Type-C adapter to connect to the USB Type-C port on the K165 or K175 device.
2. Reboot the device.
3. Press and hold **Volume Up**.

   After the boot, Avaya Vantage™ displays the Recovery menu.

   Note:

   You can navigate within the Recovery menu using the following buttons:

   - To navigate between menu options, press **Volume Up** or **Volume Down**.
   - To select the menu option, press and hold **Volume Up** or **Volume Down**.
4. Tap **Enter BRM** to navigate to Avaya Vantage™ boot recovery options.
5. Enter the administrator password using the external USB keyboard connected to the device.

Avaya Vantage™ starts the boot recovery procedure and displays a list of options.

6. Select one of the following options:
   - **Reboot**: Stops the boot recovery procedure and reboots the device.
   - **Clear phone** : Resets the device to its factory settings.
   - **Erase /cache only**: Erases the cache partition of the device that is primarily used to store recovery logs and temporary files.
   - **Erase /data only**: Erases the data stored on the device.
   - **Swap memory banks**: Swaps the boot banks on the device so the primary boot bank becomes the secondary boot bank. Avaya Vantage™ always has 2 copies of firmware:
     - Current firmware. Avaya Vantage™ uses this firmware to boot up.
     - Previously installed firmware. This firmware is updated every time the firmware on the device is upgraded.
   - **Force SELinux Permissive mode**: Starts the system with SELinux in Permissive mode. When Permissive mode is enabled, the SELinux security policy is disabled, but the system still logs all events related to the security policy.

Software distribution packages cannot be uploaded using the Utility Server

Condition

You might experience issues uploading the Avaya Vantage™ software distribution zip file to the Utility Server, which is embedded in Avaya Aura® Device Services. The Utility Server web interface has a file upload limit of 800 MB. The size of the software distribution package that is meant for K155, K165, and K175 combined is approximately 1 GB.

Solution

1. Use the **scp** command to copy the software package file to the `/tmp` directory on Utility Server.

   Example:

   ```
   scp /<path/to/source-file> <user>@<UtilityServer_HostName>:/tmp/
   ```

2. Log on to the Utility Server administrator web interface.
3. Click the **Manage Phone Firmware** link.

   The web interface lists the software package file that you copied to the `/tmp` directory.

4. Unzip and activate the Avaya Vantage™ software package.

   For more information about working with the Utility Server web interface, see *Administering Avaya Aura® Device Services*.

Video is not available

Condition

Video is not visible during calls.

Solution

1. Do one of the following:
   - If your deployment uses Avaya Aura®, ensure that the endpoint is configured with video enabled in System Manager and Communication Manager.

     From the list of features, enable **IP Softphone** and **IP Video Softphone**.
   - If your deployment uses IP Office, ensure that the IP Office server is configured to support video.
2. In the settings file, set ENABLE_VIDEO to `1`.

   In an IP Office deployment, if this parameter is not in the automatically generated settings file, configure it in the `46xxspecials.txt` file.

Video remains stuck after it is resumed

Condition

In an Avaya Aura® environment, video is paused and then resumed. The video remains stuck for one or two minutes even after it is resumed.

Solution

In Communication Manager, on the system-parameters feature form, set **Long Hold Call Timer (seconds)** to `0`.

Screen lock is enabled but the swipe to unlock action does not prompt for the password

Condition

Screen lock is enabled on Avaya Vantage™. However, when you swipe up on the Lock screen, the device is unlocked without any prompt for the password.

Solution

- In the settings file, set ENABLE_PHONE_LOCK to `1`.
- Ensure that the password for the SIP extension that you use to log on to the device contains a minimum of 5 characters.

If the SIP extension password length is less than 5 characters, the device does not get locked.

- To activate the Lock screen in the Kiosk mode, add the “com.android.systemui” package to the application list in the PIN_APP value.

  Example:

```
SET PIN_APP
“com.avaya.endpoint.avayakiosk,com.avaya.android.vantage.basic,com.avaya.endpoint.lo
gin,com.android.systemui”
```

The device displays a security certificate error

Condition

After the device boots up, it displays a security certificate error. The problem persists after subsequent reboots.

Cause

Some required certificates might not be downloaded to the device through the TRUSTCERTS parameter.

Solution

1. Check the following to ensure that you have defined the TRUSTCERTS parameter correctly for the required certificate files to be downloaded to the device:
   - Check and ensure all required certificates for services to be run on the device are included in the list of certificates defined in the TRUSTCERTS parameter.
   - Ensure that URLs or file paths to the certificate files are correctly defined in the TRUSTCERTS parameter value.
   - Ensure that the TRUSTCERTS parameter value does not exceed the limit of 1024 characters for firmware release 2.1 or earlier. For firmware release 2.2 and later, the length of the parameter value can be up to 4000 characters.

     Tip:

     Avoid using long absolute URLs to the certificate files. Instead, copy the files to the file server and provide relative file paths.
   - When using Avaya Aura® Device Services, ensure that the TRUSTCERTS parameter value defined in the `46xxsettings.txt` file has the same set of certificates as the value defined in Avaya Aura® Device Services. However, the syntax does not need to be the same. The certificate file paths or the order of the certificates in the list need not be the same in the parameter value in the `46xxsettings.txt` file and Avaya Aura® Device Services. When using Avaya Aura® Device Services, you must use absolute file paths in the parameter value.

   For more information about defining the TRUSTCERTS parameter, see Certificate configuration parameters on page 281.
2. After updating the configuration, reboot the device.

H.323 contacts are downloaded without a phone number

Condition

When downloading contacts through PPM, H.323 contacts are saved with only a name, but no phone number. Therefore, you cannot click on the contact to make a call.

Solution

You must add the phone number for the contact manually before you can make a call.

Some applications do not support Android 8.1

Condition

Some Android applications do not function as expected after the Avaya Vantage™ firmware is upgraded to Release 2.0.1. These applications do not support Android 8.1 and can only run on Android 6.x.

Important:

Avaya Vantage™ Connect Release 2.0.1 is only supported with Avaya Vantage™ Release 2.0.1 firmware. Earlier Avaya Vantage™ firmware versions are not supported. You can only install Avaya Vantage™ Connect 2.0.1 on an Avaya Vantage™ device with Android 8.1.

Solution

Downgrade the Avaya Vantage™ firmware to Release 2.0 so that the Android OS is also downgraded to 6.0.1.

1. Ensure that upgrade parameters, such as UPGRADE_POLICY and UPGRADE_POLLING_PERIOD, are set correctly in the settings file.
2. Save the updated settings file on the file server.
3. Ensure that the Avaya Vantage™ device is pointing to the correct file server.
4. Download the Release 2.0 firmware distribution package to the file server.

   Avaya Vantage™ automatically performs a factory data reset. This is a software-triggered factory reset, which cannot be avoided. At the next polling period, Avaya Vantage™ downloads the Release 2.0 upgrade files and installs the files according to the configured upgrade policy.
5. Re-configure the Avaya Vantage™ device as required.

   If it is not done automatically, you must set up the file server. You must also add any required accounts, such as your Google account.

Some applications are not downgrading on K175 with Android 8.1

Condition

On the Avaya Vantage™ K175 device with Android 8.1, some applications, such as Avaya IX™ Workplace Client, do not downgrade to an earlier release through the PUSH_APPLICATION method. Instead, the current release of the application remains on the device.

Solution

1. Uninstall the existing application version:
   a. In the `46xxsettings.txt` file, from the `SET PUSH_APPLICATION` command string, delete the path to the application.
   b. Save the file.

      On the next polling period, the application is uninstalled from the device. If you want to implement this change immediately, you can reboot the device.

   Warning:

   Uninstalling results in the loss of application data.
2. After the application is uninstalled, push the earlier release of the application to the device:
   a. In the `46xxsettings.txt` file, in the `SET PUSH_APPLICATION` command string, add the path to the application APK file that you want to install.
   b. Save the file.

      On the next polling period, Avaya Vantage™ downloads the settings file and the application package, and installs the application on the device. If you want to implement this change immediately, you can reboot the device.

Call is stuck after the port switch is set to forceUnauthorized

Condition

During an active call, when you set the port switch to `forceUnauthorized`, the call becomes unresponsive and you cannot end it.

Cause

Setting the port switch to `forceUnauthorized` causes a network failure, but it might take time for the device to detect that it is not connected to Session Manager.

Solution

You can only end the call after the device detects the timeout.

Important:

To prevent disruptions, avoid changing settings during office hours. Wait until off-hours.

Cannot join a conference bridge when DTMF is set to in-band

Condition

In an IP Office environment, you cannot dial the access code required to enter a conference bridge.

Cause

In-band DTMF digits are not supported. This issue occurs when DTMF is set to in-band in IP Office.

Solution

Use out-of-band DTMF digits (RFC 2833).

Cannot find application package names for Kiosk mode

Condition

You want to pin an Android application to the Avaya Vantage™ Home screen in Kiosk mode, but you do not know the package name.

Solution

Use one of the following methods to find the package name of a third-party Android application:

- Find the application URL on the Google Play Store application or website. The package name is at the end of the URL after `?id=`.

  For example, in the application URL for Google Chrome, `https://play.google.com/store/apps/details?id=com.android.chrome`, the package name is *com.android.chrome*.

  For more information, see www.techmesto.com/find-android-app-package-name.

- Install a package viewer application from Google Play Store and use it to find the package name of an application installed on your device.

For a list of package names of Avaya applications that are pre-installed or pushed onto the device, see Applications to pin in Kiosk mode on page 142.

Chapter 16: Resources

Documentation

See the following related documents at http://support.avaya.com. Many of these documents are also available at http://documentation.avaya.com/.

Title	Use this document to:	Audience
Overview		
Avaya Aura® Session Manager Overview and Specification	Understand characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security, and licensing requirements of Avaya Aura® Session Manager.	• Customers • Sales, services, and support personnel
Deploying		
Installing and Administering Avaya Vantage™ in an Open SIP Environment	Install, configure, and maintain Avaya Vantage™ in an Open SIP environment.	Implementation personnel and administrators
Deploying Avaya Aura® Session Manager	Deploy Avaya Aura® Session Manager.	Implementation personnel and service administrators
Deploying Avaya Aura® System Manager on System Platform	Deploy Avaya Aura® System Manager.	Implementation personnel and service administrators
Deploying Avaya Aura® Conferencing: Basic Installation	Deploy Avaya Aura® Conferencing.	Implementation personnel and service administrators
Avaya IP Office™ Platform SIP Telephone Installation Notes	Deploy SIP endpoints on IP Office.	Implementation personnel and service administrators
Administering		
Administering Avaya Aura® Session Manager	Administer and maintain Avaya Aura® Session Manager.	System administrators

Table continues…

Title	Use this document to:	Audience
Upgrading Avaya Aura® Session Manager	Upgrade Avaya Aura® Session Manager.	System administrators
Administering Avaya Aura® Conferencing	Administer Avaya Aura® Conferencing.	System administrators
Administering Avaya Session Border Controller for Enterprise	Administer Avaya Session Border Controller for Enterprise.	System administrators
Administering Avaya IP Office™ Platform with Manager	Perform administration tasks using IP Office Manager.	System administrators
Maintaining		
Maintaining Avaya Aura® Session Manager	Maintain Avaya Aura® Session Manager.	System administrators and IT personnel
Troubleshooting Avaya Aura® Session Manager	Troubleshoot known issues for Avaya Aura® Session Manager.	System administrators and IT personnel
Using		
Using the Avaya Vantage™ Device	Use the Avaya Vantage™device.	• End users • Support personnel
Using Avaya Vantage™ Connect	Use the Avaya Vantage™ Connect application.	End users
Using Avaya IX™ Workplace Client for Android, iOS, Mac, and Windows	Use Avaya IX™ Workplace Client.	• End users • Support personnel
Using Avaya Device Enrollment Services to Manage Endpoints	Use Device Enrollment Services to manage endpoints or devices.	Non-Avaya users, including service providers and resellers

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.

6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.

7. Click **Enter**.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **My Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add content from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

  Navigate to the **My Content** > **Watch list** menu, and do the following:
  - Set how frequently you want to be notified, starting from every day to every 60 days.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

Training

The following course is available on the Avaya Learning website at http://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field and press**Enter** to search for the course.

Course code	Course title
60061W	Installing and Administering Avaya Vantage™ Devices

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://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.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Appendix A: Supported configuration parameters

Parameters for controlling configuration parameter downloads

Parameter	Type	Default value	Is set to default on reset	Description
GROUP	Numeric	0	Yes	Group identifier to download a specific configuration set for a dedicated user group during startup. The range is from 0 to 999. The parameter can be used in conditional statements in the `46xxsettings.txt` settings file. For provisioning, use the **Settings** > **Network & Internet** > **More** > **Group** menu on the device.
AUTH	Numeric	0	No	Authentication flag for all file downloads, including configuration and image files, and Avaya Aura® Device Services configuration retrieval. Assign one of the following values: • 0: Secure file downloading is not required. Avaya Vantage™ downloads firmware and configuration files from HTTP or HTTPS servers. • 1: Secure file downloading is required. Avaya Vantage™ downloads firmware and configuration files from HTTPS servers only. For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.

Phone parameters

Parameter	Type	Default value	Is set to default on reset	Description
MODEL	String	Factory settings	No	Model identifier of the telephone, which includes the first 8 characters of the telephone's apparatus code. The length ranges from 8 to 10 ASCII characters. This parameter can be used in conditional statements in the `46xxsettings.txt` file. You cannot modify the parameter value.

MODEL4	String	Factory settings	No	Name of the device model or the truncated model identifier.
				You cannot modify this parameter value.
				This parameter can have one of the following values depending on the device model:
				• K175 for the standard Avaya Vantage™ device with a camera.
				• K165 for the standard Avaya Vantage™ device without a camera.
				• K155 for the Avaya Vantage™ device with a small screen and a physical keypad.
				You can use this parameter in conditional statements in the `46xxsettings.txt` file.
				An example of using the MODEL4 parameter in the `46xxsettings.txt` file:
				`IF $MODEL4 SEQ K155 GOTO K155SW`
				`IF $MODEL4 SEQ K175 GOTO K175SW`
				`GOTO GETSET`
				
				`# K155SW`
				`SET ACTIVE_CSDK_CSDK_BASED_PHONE_APP "com.avaya.android.vantage.basic"`
				`GOTO GETSET`
				
				`# K175SW`
				`SET ACTIVE_CSDK_CSDK_BASED_PHONE_APP "com.avaya.android.flare"`
				`GOTO GETSET`

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
MACADDR	String	Factory settings	No	Media Access Control (MAC) address of the device. MACADDR always refers to the Ethernet MAC address. MACADDR contains six pairs of ASCII hexadecimal characters separated by colons. This parameter can be used in conditional statements in the `46xxsettings.txt` file.

General phone functionality settings

Audio parameters

Parameter	Type	Default value	Is set to default on reset	Description
BRANDING_VOLUME	Numeric	5	Yes	Specifies the playback level of the Avaya audio branding tone, which plays when you log in or unlock the device. The parameter value can be from 0 to 8: • 8: 9 db above nominal • 7: 6 db above nominal • 6: 3 db above nominal • 5: nominal • 4: 3 db below nominal • 3: 6 db below nominal • 2: 9 db below nominal • 1: 12 db below nominal • 0: No audio branding tone For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description

RINGTONES	String	Null		Specifies a list of audio files to be downloaded as ring tones and offered to users for selection.
				
				The list can contain 0 to 1023 octets of UTF-8 characters.
				
				Values are separated by commas without any intervening spaces. If the audio files are stored in the same directory configured in FILE_SERVER_URL, you can list the file names in the following format: `ring1.wav,ring2.wav,ring3.mp3,rin4.ogg`. If the file is stored in a different location, then use the tuple format: *`<Filename with sufix>=<path>/<filename>`*. For example: `name.ogg=URI`.
				
				If you are using `.mp3` or `.ogg` files that include the ID3 metadata container with a non-empty title field, the title field is displayed by Android in the list of ringtones. If the `.mp3` or `.ogg` file includes a metadata container with an empty title field, the file name is displayed. If a `.wav` file is used, the filename is always presented.
				
				When using the tuple format, the file name must include the audio file suffix. Changing the file suffix only with the same file name will not trigger a new download.
				
				For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.
				
				For example:
				
				`SET RINGTONES “swhistle.wav,chorn.wav,ring4.mp3”`
				
				`SET RINGTONES “swhistle.wav=tones/swhistle.wav,ring4.mp3=mp3files/ring4.mp3”`

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
RINGTONESTYLE	Numeric	0		Specifies the style of ring tones. Assign one of the following values: • 0: North American ring tones are available (default). • 1: European ring tones are available. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Video parameters

Parameter	Type	Default value	Is set to default on reset	Description
CAMERASTAT	Numeric	1		Controls whether the device user can enable or disable the integrated camera and the external third-party USB camera, if connected to the device, through the **Settings** menu. Assign one of the following values: • 0: Camera is disabled. The device user has no option to enable or disable the camera through the **Settings** menu. • 1: Camera is enabled. The device user has no option to enable or disable the camera through the **Settings** menu. • 2: The device user can enable or disable the camera through the **Settings** menu. When the camera is disabled, you can still see video from other users, but Android applications cannot transmit video from your camera. You also cannot take photos or video clips. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

Device UI related settings

Common UI operation

Parameter	Type	Default value	Is set to default on reset	Description
BACKLIGHT_SELECTABLE	Numeric	1	Yes	Specifies whether the device sleep time is determined by you, as the administrator, or through user configuration. After the device is idle for the specified sleep time, the device display backlight is turned off. You can assign one of the following values: • 0: To obtain the device idle time value from the BAKLIGHTOFF parameter you set in the `46xxsettings.txt` file. • 1: To enable the user to set the idle time value using the **Sleep** option in the **Settings** > **Display** menu. For provisioning, use: • The **`SET`** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.
BAKLIGHTOFF	Numeric	10	Yes	Specifies the idle time in minutes, after which the device turns off the display backlight or activates the screen saver. The range is from 0 to 999. A value of 0 means that the display backlight is not turned off automatically when the phone is idle. This parameter is only applicable when BACKLIGHT_SELECTABLE is set to 0. For provisioning, use: • The **`SET`** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
ADMIN_INITIAL_SCREEN	String	PHONE	Yes	This parameter specifies whether Avaya Vantage™ presents the Home screen of the device or the Avaya™ Client SDK telephony application as the initial screen after the user logs in manually or unlocks the device using the quick unlock feature. This parameter is not applicable for automatic login. Avaya Vantage™ only uses this parameter when the **Settings** > **Display** > **Screen presented after login or quick unlock** field is set to **Admin default**, which is the default setting. Assign one of the following values: • HOMESCREEN: The device Home screen is presented as the initial screen. • PHONE: The Avaya™ Client SDK telephony application is presented as the initial screen. For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.
DARK_BOOTUP	Numeric	0	Yes	Specifies whether the display backlight is turned off when Avaya Vantage™ starts up to avoid any visual disturbance, especially during night time. Assign one of the following values: • 0: The device does a regular start-up with the display backlight turned on. • 1: The device does a dark start-up with the display backlight turned off immediately after reboot. You cannot see start-up screens unless you pick up the handset, touch the screen or hard key buttons, or an incoming call arrives. For provisioning, use: • The **`SET`** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

Specific audio settings

Parameter	Type	Default value	Is set to default on reset	Description
HEADSETBIDIR	Numeric	0	Yes	Specifies whether bidirectional signaling is supported on the headset interface. Bidirectional signalling allows you to forward off-hook events and incoming call alerts from Avaya Vantage™ to a headset when a headset base station is connected to the headset connector. Assign one of the following values: • 0: Disabled. • 1: Switch hook and alert signaling are both enabled. • 2: Only switch hook signaling is enabled. **Important:** This parameter must only be used when using a wireless headset if the base station is connected to the headset connector of the device. In other cases, such as when using a wired headset, the value must be set to 0. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** > **Sound & Audio & Camera** > **Audio settings** > **Headset signaling** menu on the device. This parameter can be stored on the PPM or backup server.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
AGCHAND	Numeric	0	No	Specifies Automatic Gain Control (AGC) for the handset. The options are: • 0: AGC is disabled. • 1: AGC is enabled. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** > **Sound & Audio & Camera** > **Audio settings** > **Auto gain control (AGC)** > **Handset Auto Gain Control** menu on the device. This parameter can be stored on the PPM or backup server.
AGCHEAD	Numeric	0	No	Specifies Automatic Gain Control (AGC) for the headset. The options are: • 0: AGC is disabled. • 1: AGC is enabled. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** > **Sound & Audio & Camera** > **Audio settings** > **Auto gain control (AGC)** > **Headset Auto Gain Control** menu on the device. This parameter can be stored on the PPM or backup server.
AGCSPKR	Numeric	0	No	Specifies Automatic Gain Control (AGC) for the speaker. The options are: • 0: AGC is disabled. • 1: AGC is enabled. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** > **Sound & Audio & Camera** > **Audio settings** > **Auto gain control (AGC)** > **Speaker Auto Gain Control** menu on the device. This parameter can be stored on the PPM or backup server.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
AUDIOSTHD	Numeric	0	Yes	Specifies headset sidetone settings. The options are: • 0: Normal level. • 1: Three levels softer than normal. • 2: Off (inaudible). • 3: One level softer than normal. • 4: Two levels softer than normal. • 5: Four levels softer than normal. • 6: Five levels softer than normal. • 7: Six levels softer than normal. • 8: One level louder than normal. • 9: Two levels louder than normal. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
AUDIOSTHS	Numeric	0	Yes	Specifies handset sidetone settings. The options are: • 0: Normal level. • 1: Three levels softer than normal. • 2: Off (inaudible). • 3: One level softer than normal. • 4: Two levels softer than normal. • 5: Four levels softer than normal. • 6: Five levels softer than normal. • 7: Six levels softer than normal. • 8: One level louder than normal. • 9: Two levels louder than normal. This parameter is supported by wired handsets only. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
HEADSET_PROFILE	Numeric	0	Yes	Specifies the headset audio profile selected by the user. The range is from 0 to 20. If the value of HEADSET_PROFILE is 0, the headset audio profile is not selected. For provisioning, use the **Settings** > **Sound & Audio & Camera** > **Audio settings** > **Headset profile** menu on the device. This parameter can be stored on the PPM or backup server.
HEADSET_PROFILE_DEFAULT	Numeric	1	Yes	Specifies the number of the default headset audio profile. The range is from 1 to 20. For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.
HEADSET_PROFILE_NAMES	String	Null	Yes	Specifies names to be displayed for headset audio profile selection. The value of the parameter is a list of profile names separated by commas without any spaces between entries. If profile names include spaces, the list must use quotations. Names must not contain commas or double quote characters. To retain the default name of a specific profile, do not provide a new name for the profile. The parameter can contain up to 0 to 255 octets of UTF-8 characters. For provisioning, use the **`SET`** command in the `46xxsettings.txt` file. For example, to rename the first and third profiles and to retain the default name of the second profile, enter the following: `SET HEADSET_PROFILE_NAMES "Profile 1,,Profile 3"`

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
HANDSET_PROFILE	Numeric	0	Yes	Specifies the handset audio profile selected by the user. The range is from 0 to 20. If the value of HANDSET_PROFILE is 0, the handset audio profile is not selected. For provisioning, use the **Settings** > **Sound & Audio & Camera** > **Audio settings** > **Handset profile** menu on the device. This parameter can be stored on the PPM or backup server.
HANDSET_PROFILE_DEFAULT	Numeric	1	Yes	Specifies the number of the default handset audio profile. The range is from 1 to 20. For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.
HANDSET_PROFILE_NAMES	String	null string	Yes	Specifies names to be displayed for handset audio profile selection. The value of the parameter is a list of profile names separated by commas without any spaces between entries. If profile names include spaces, the list must use quotations. Names must not contain commas or double quote characters. To retain the default name of a specific profile, do not provide a new name for the profile. The parameter can contain up to 0 to 255 octets of UTF-8 characters. For provisioning, use the **`SET`** command in the `46xxsettings.txt` file. For example, to rename the first and third profiles and to retain the default name of the second profile, enter the following: `SET HANDSET_PROFILE_NAMES “Profile 1,,Profile 3”`

Display settings for the Home screen

Parameter	Type	Default value	Is set to default on reset	Description
LOGOS	String	“”	Yes	Specifies a list of custom logo definitions or wallpapers that can be used as a background on the display. Each entry in the list is a logo label followed by an equal sign (=) followed by a logo file name or URL. Entries are separated by commas without any intervening spaces. The logo URL can be specified using either absolute or relative format. If the relative format is used, the origin is the directory specified by FILE_SERVER_URL. Avaya Vantage™ supports the following file types: PNG, JPG (JPEG), GIF, and BMP. GIF is presented without animation. Use an image that fits the entire device screen and appears on all pages. • For K175 devices, the screen is 8 inches with a resolution of 800 x 1280 (width x height) pixels. • For K155 devices, the screen is 5 inches with a resolution of 1280 x 720 (width x height) pixels. For provisioning, use the **SET** command in the `46xxsettings.txt` file. For example: `SET LOGOS “Red Balloon=redballoon.jpg,Blue Balloon=https://123.123.7.8/blueballoon.jpg,Purple=../purple.jpg”`

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
CURRENT_LOGO	String	“”	Yes	Specifies the background image to display on Avaya Vantage™. The value of the parameter is one of the logo labels specified in the LOGOS parameter. When the value is “”, the default logo or wallpaper is displayed. For provisioning, use the **SET** command in the `46xxsettings.txt` file. For example: If LOGOS is defined as `“Red Balloon=redballoon.jpg,Blue Balloon=blueballoon.jpg”`, then you can set CURRENT_LOGO as one of the following: • `SET CURRENT_LOGO “Red Balloon”` • `SET CURRENT_LOGO “Blue Balloon”`

Screen saver display settings

Parameter	Type	Default value	Is set to default on reset	Description
SCREENSAVER_IMAGE_SELECTABLE	Numeric	1		Specifies whether device users can set up a screen saver of their choice locally from the device **Settings** menu. You can assign one of the following values: • 0: To disable the screen saver selection option for device users. • 1: To enable the screen saver selection option for device users.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
SCREENSAVER_IMAGE	String	“”		Specifies a list of custom screen saver images to be downloaded to Avaya Vantage™. The parameter value can be a comma-separated list of screen saver image URLs. The list entries are separated by commas without any intervening spaces. You can specify a URL using the absolute or relative format. For the relative format, the origin is the directory specified by FILE_SERVER_URL. Avaya Vantage™ supports the following file types: PNG, JPG (JPEG), GIF, and BMP. GIF is presented without animation. Use an image that fits the entire device screen. • For K175 devices, the screen is 8 inches with a resolution of 800 x 1280 (width x height) pixels. • For K155 devices, the screen is 5 inches with a resolution of 1280 x 720 (width x height) pixels. Example: `SET SCREENSAVER_IMAGE “redballoon.jpg,https://123.234.5.6/blueballoon.jpg”`
SCREENSAVER_IMAGE_DISPLAY	String	“”		Specifies the custom screen saver image to be displayed on Avaya Vantage™. The image file name must be the same as one of the file names you listed in SCREENSAVER_IMAGE. If you set SCREENSAVER_IMAGE_SELECTABLE to 1, then device users can override this custom screen saver with a screen saver of their choice through the device **Settings** menu. If you do not set a screen saver image or set the wrong file name in this parameter, device users see a black screen as the custom screen saver. Example: `SET SCREENSAVER_IMAGE_DISPLAY redballoon.jpg`

Language and country settings

Parameter	Type	Default value	Is set to default on reset	Description
ISO_SYSTEM_LANGUAGE	String	en_US	Yes	Specifies the device system language. ISO_SYSTEM_LANGUAGE uses the `LL[_CC]` format where: • `LL` is a language code. The language code is represented by two lowercase letters. For example: `en`. For more information about codes, see ISO 639-1. • `CC` is an optional country code. The country code is represented by two uppercase letters. For example: `GB`. For more information about codes, see ISO 3166-1. If you use an optional country code, then the language code and the country code must be separated by the underscore symbol. For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.
COUNTRY	String	USA	Yes	Specifies a country where Avaya Vantage™ is used. This parameter is used for country-specific Wi-Fi and anti-flickering frequency settings. If Avaya Vantage™ cannot identify the country specified in the parameter, it applies default settings. For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.

Date and time settings

Parameter	Type	Default value	Is set to default on reset	Description
TIMEZONE	String	Etc/GMT	Yes	Specifies the time zone in the Olson name format. For example: `America/New_York`. For more information about the name format and for a list of time zones, see the Time Zone Database. For provisioning, use: • DHCP option 242. • The **SET** command in the `46xxsettings.txt` file. With IP Office, set this parameter in the `46xxspecials.txt` file.
ADMINTIMEFORMAT	Integer	0	Yes	Specifies whether Avaya Vantage™ uses the 12-hour or 24-hour time format. The options are: • 0: Use the 12-hour time format. • 1: Use the 24-hour time format. Avaya Vantage™ uses the selected time format in all areas that displays time, including the top bar, call log, and calendar. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** menu on the device. • The settings file received from Avaya Aura® Device Services.

Server addresses and ports

Parameter	Type	Default value	Description
DNSSRVR	String	0.0.0.0	Specifies up to three IP addresses of DNS servers. Use either an IPv4 or IPv6 address. The value of the parameter is a list of IP addresses separated by commas without any spaces between entries. Avaya Vantage™ tries to connect to the DNS servers in the order specified in the parameter. Both the Wi-Fi and Ethernet interfaces use the configured DNS server and domain information. An option to configure DNS information specifically for each Wi-Fi network is unavailable. Therefore, if a user toggles between the Wi-Fi and Ethernet interfaces, then the configured DNS information is applicable for both interfaces. For provisioning, use: • The Option 6 value in a DHCPACK message. • A `name=value` pair in DHCPv6 Reply VSI option 242. • The **`SET`** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. • The **Settings** menu on the device.
DOMAIN	String	Null	Specifies a domain name. Avaya Vantage™ uses domain names when DNS names in configuration parameter values are resolved to IP addresses. If DOMAIN is null, all DNS names must be fully qualified. If servers in a network are in more than one sub-domain, server DNS names must include the sub-domain name and DOMAIN must be set to the lowest level common domain. For provisioning, use: • The Option 15 value in a DHCPACK message. • A `name=value` pair in DHCPv6 Reply VSI option 242. • The **`SET`** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
FILE_SERVER_URL	String	Null	Specifies the file server URLs for downloading firmware and configuration files. Avaya Vantage™ tries to connect to file servers in the order specified in the parameter. The value of the parameter is a list of file server addresses separated by commas without any spaces between entries. A file server URL must use one of the following formats: • `http://hostname[:port][/path]` • `https://hostname[:port][/path]` Where: • `hostname` is an IPv4 or IPv6 address, or an FQDN. Encapsulate an IPv6 address in square brackets. • `port` is an optional port number. • `path` is an optional path to a directory where distribution packages and other files are stored. You can provide URLs of HTTP servers without the leading `http://`. You must explicitly specify `https://` for HTTPS servers. The default port for HTTP is 80. The default port for HTTPS is 443. The parameter supports `$MACADDR`, `$MODEL4`, and `$SERIALNO` as part of the directory path in the FILE_SERVER_URL value. The device replaces these strings with the relevant MAC address, MODEL4, and serial number information in capital letters. The device uses the MAC address value without any colons. For example, if you configure the value of FILE_SERVER_URL as “http://example.com/$MODEL4dir”, then all K175 devices will use “http://example.com/K175dir” as the file server address. The K175 devices will download files with relative paths from If this parameter is set, Avaya Vantage™ ignores the HTTPSRVR, HTTPPORT, HTTPDIR, TLSSRVR, TLSSRVRDIR, and TLSPORT parameters. For provisioning, use: • LLDP Avaya/Extreme Proprietary File Server TLV. The precedence is 1. • DHCP option 43. The precedence is 2. • A `name=value` pair in DHCPv6 Reply VSI option 242. The precedence is 2.

Table continues…

Parameter	Type	Default value	Description
			• A `name=value` pair in a DHCPACK message. The precedence is 2. • The siaddr field value in the DHCPACK message. The precedence is 2. Only the dotted decimal format is supported. Avaya Vantage™ considers addresses received using this method as HTTP server addresses. • The **SET** command in the `46xxsettings.txt` file. The precedence is 3. • The **Settings** menu on the device. The precedence is 5.
HTTPPROXY	String	Null	Specifies an address of an HTTP proxy server. A proxy server address uses the `hostname[:port]` format, where: • `hostname` is either an IP address in the dot-decimal format or a fully-qualified domain name. • `port` is an optional port number. This parameter is not a URL. Therefore, you must not begin the value with `http://`. The range is the default string length. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** menu on the device.
HTTPEXCEPTIONDOMAINS	String	Null	Specifies domains that are excluded for use of the HTTP proxy server. The value of the parameter is a list of domains separated by commas without any spaces between entries. The range is the default string length. A HTTP connection for SCEP is set up through HTTPPROXY only if the rightmost part of the domain specified in MYCERTURL does not match any domain specified in this parameter. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** menu on the device.

Table continues…

Parameter	Type	Default value	Description
HTTPSRVR	String	0.0.0.0	Specifies a list of HTTP file server addresses in the IPv4, IPv6, or DNS name format. The device uses these servers for downloading firmware and configuration files. Avaya Vantage™ uses this parameter only if FILE_SERVER_URL and TLSSRVR are not set. The value of the parameter is a list of HTTP file server addresses separated by commas without any spaces between entries. The value can contain up to 255 ASCII characters. • LLDP Avaya/Extreme Proprietary File Server TLV. The precedence is 1. • DHCP option 43. The precedence is 2. • A `name=value` pair in a DHCPACK message. The precedence is 2. • The siaddr field value in the DHCPACK message. The precedence is 2. Only the dotted decimal format is supported. • A `name=value` pair in DHCPv6 Reply VSI option 242. The precedence is 2. • The **`SET`** command in the `46xxsettings.txt` file. The precedence is 3.

Table continues…

Parameter	Type	Default value	Description
TLSSRVR	String	0.0.0.0	Specifies a list of HTTPS file server addresses in the IPv4, IPv6, or DNS name format. The device uses these servers for downloading firmware and configuration files. Avaya Vantage™ uses this parameter only if FILE_SERVER_URL is not set. The value of the parameter is a list of HTTPS file server addresses separated by commas without any spaces between entries. The value can contain up to 255 ASCII characters. For provisioning, use: • LLDP Avaya/Extreme Proprietary File Server TLV. The precedence is 1. • DHCP option 43. The precedence is 2. • A `name=value` pair in a DHCPACK message. The precedence is 2. • A `name=value` pair in DHCPv6 Reply VSI option 242. The precedence is 2. • The **`SET`** command in the `46xxsettings.txt` file. The precedence is 3. • The settings file received from Avaya Aura® Device Services. The precedence is 4.

Table continues…

Parameter	Type	Default value	Description
HTTPDIR	String	Null	Specifies a path to the directory of the HTTP file server where configuration files and software images are stored. This path is relative to the URL of the HTTP file server. Avaya Vantage™ prepends the parameter value to all file names used in HTTP **GET** operations. Avaya Vantage™ uses this parameter only if you configure HTTPSRVR and do not configure FILE_SERVER_URL and TLSSRVR. The parameter value can contain up to 127 characters. The parameter supports `$MACADDR`, `$MODEL4`, and `$SERIALNO` as part of the path in the HTTPDIR value. The device replaces these strings with the relevant MAC address, MODEL4, and serial number information in capital letters. The device uses the MAC address value without any colons. For example, if you configure HTTPDIR as “$MODEL4dir”, then all K175 devices will download files with relative paths from “K175dir”. Do not use this parameter in configurations where files are stored in the default directory of the HTTP server URL. For provisioning, use: • A `name=value` pair in a DHCPACK message. • DHCP option 43. • The **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
TLSDIR	String	Null	Specifies a path to the directory of the HTTPS file server where configuration files and software images are stored. This path is relative to the URL of the HTTPS file server. Avaya Vantage™ prepends this parameter value to all file names used in HTTPS **GET** operations. Avaya Vantage™ uses this parameter only if you configure TLSSRVR and do not configure FILE_SERVER_URL. The parameter value can contain up to 127 characters. The parameter supports `$MACADDR`, `$MODEL4`, and `$SERIALNO` as part of the path in the TLSDIR value. The device replaces these strings with the relevant MAC address, MODEL4, and serial number information in capital letters. The MAC address value is used without any colons. For example, if you configure TLSDIR as “$MODEL4dir”, then all K175 devices will download files with relative paths from “K175dir”. For provisioning, use: • A `name=value` pair in a DHCPACK message. • DHCP option 43. • The **SET** command in the `46xxsettings.txt` file.
HTTPPORT	Numeric	80	Specifies the destination TCP port for HTTP requests. The range is from 0 to 65535. Avaya Vantage™ uses this parameter only if FILE_SERVER_URL is not set. For provisioning, use: • A `name=value` pair in a DHCPACK message. • DHCP option 43. • The **SET** command in the `46xxsettings.txt` file.
TLSPORT	Numeric	443	Specifies the destination TCP port for HTTPS requests. The range is from 0 to 65535. Avaya Vantage™ uses this parameter only if FILE_SERVER_URL is not set. For provisioning, use: • A `name=value` pair in a DHCPACK message. • DHCP option 43. • The **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
SIP_CONTROLLER_LIST	String	Null	Specifies a list of IP addresses of SIP proxy or registrar servers. The entries in the list are separated by commas without any spaces between entries. Each entry in the list has the following format: `host[:port][;transport=xxx]`, where: • `host` is an IP address in the dot-decimal (IPv4), colon-hex (IPv6), or DNS format. Avaya Vantage™ supports IPv6 addresses only in the Avaya Aura® environment. • `port` is the optional port number. If the port number is not specified, Avaya Vantage™ uses the following default values: - 5060 for TCP - 5061 for TLS If you are providing the port number with an IPv6 address, encapsulate the IPv6 address in square brackets. • `transport` is the optional transport type. The supported options are TLS, TCP, or UDP. If the transport type is not specified, Avaya Vantage™ uses TLS as the default transport type. Avaya Vantage™ supports UDP only in an Open SIP environment. In the Avaya Aura® environment, set the transport protocol as TLS. Avaya does not recommend to use TCP with Avaya Aura®. **Important:** To avoid multiple registrations to the same SIP controller over IPv4 and IPv6 addresses, you must specify *only* an IPv4, IPv6, or FQDN address for each SIP controller in SIP_CONTROLLER_LIST through all provisioning sources. When the SIP controller is in dual-stack mode, specify only FQDN of the controller in the list. Do not specify mix of IPv4 and IPv6 addresses for the same SIP controller. The parameter value can have up to 255 characters. This parameter is *not* supported in the non Avaya™ Client SDK application based mode.

Table continues…

Parameter	Type	Default value	Description
			For provisioning, use: • LLDP Avaya/Extreme Proprietary Call Server TLV. The precedence is 1. • A `name=value` pair in a DHCPACK message. The precedence is 3. • DHCP option 43. The precedence is 3. • A `name=value` pair in DHCPv6 Reply VSI option 242. The precedence is 3. • The **`SET`** command in the `46xxsettings.txt` file. The precedence is 4. • The settings file received from Avaya Aura® Device Services. • The value stored on the PPM or backup server. The precedence is 5. • The **Settings** menu on the device. The precedence is 5. **Important:** For emergency call support when you are logged out of the device, you must configure the SIP_CONTROLLER_LIST parameter using the `46xxsettings.txt` file, DHCP, LLDP, or the **Settings** menu on the device. If you only configure SIP_CONTROLLER_LIST in Avaya Aura® Device Services, emergency calls do not work as expected.
SIPDOMAIN	String	Null	Specifies the SIP domain name used for SIP registration. The value of the parameter can have up to 255 characters. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. For provisioning, use: • The **`SET`** command in the `46xxsettings.txt` file. • The value stored on the PPM server. • The **Settings** menu on the device.

Table continues…

Parameter	Type	Default value	Description
SIMULTANEOUS_REGISTRATIONS	Numeric	3	Specifies the number of SIP proxy or registrar server instances with which the device can simultaneously register. The range is from 1 to 3. In an IP Office environment, set this parameter to 1. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ENABLE_SIP_USER_ID	Numeric	0	Specifies whether Avaya Vantage™ distinguishes between the SIP user name and the SIP user ID for SIP registration and SIP authentication respectively. The SIP user name is identical to the SIP user ID in most SIP server environment. Configure the ENABLE_SIP_USER_ID parameter when the user ID is not identical to the user name. The parameter controls the display of the field to enter the SIP user ID on the Login screen. You can assign one of the following values: • 0: The **Authentication username** field for entering the SIP user ID is not available on the Login screen. • 1: The **Authentication username** field for entering the SIP user ID is available on the Login screen. In absence of the user ID value, Avaya Vantage™ considers the user ID to be identical to the user name. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
SNTPSRVR	String	0.avaya.pool.ntp.org,1.avaya.pool.ntp.org,2.avaya.pool.ntp.org,3.avaya.pool.ntp.org,129.6.15.28,132.163.97.1	Specifies a list of Simple Network Time Protocol (SNTP) server FQDNs or IP addresses. Avaya Vantage™ uses this parameter to retrieve date and time information from SNTP servers. The value of the parameter is a list of SNTP server FQDNs or IP addresses using either the dotted decimal or DNS format. Entries in the list are separated by commas without any spaces between entries. The parameter value can contain up to 255 characters. For provisioning, use: • DHCP option 42. • The **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
USER_AUTH_FILE_SERVER_URL	String	“” (Null)	Specifies a list of user authenticated file server URLs. Currently, Avaya Vantage™ only supports Avaya Aura® Device Services as a user authenticated file server only. • If you configure this parameter, Avaya Vantage™ displays the Unified Login screen. If you did not provide the user’s SIP extension and password in Avaya Aura® Device Services, Avaya Vantage™ will also prompt the user to enter the SIP extension and password. If you set USER_AUTH_FILE_SERVER_SSO to 3, the user sees the web-view based SSO Login screen. • If you do not set this parameter, Avaya Vantage™ displays the SIP Login screen. In this case, the user only needs to enter the SIP extension and password to log in to Avaya Vantage™. The value of the parameter is a list of file server addresses separated by commas without any spaces between entries. A file server URL must use the following format: • `https://hostname[:port]` In the URL: • `hostname` is either an IP address in the dotted decimal, colon-hex, or DNS format. • `port` is an optional port number. Avaya Vantage™ supports accepts only HTTPS related URLs as this parameter value. You can provide URLs of HTTPS servers without the leading `https://`. The default port for HTTPS is 443. For provisioning, use: • A `name=value` pair in a DHCPACK message. • DHCPv6 Reply VSI option 242. • The **`SET`** command in the `46xxsettings.txt` file. • The **Settings** menu on the device.

Table continues…

Parameter	Type	Default value	Description
USER_AUTH_FILE_SERVER_SSO	Numeric	1	Specifies what authentication method is used when accessing the user authenticated file server. You can assign one of the following values • 1: Enables unified login. • 3: Enables OAuth-based SSO. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
AVAYA_AUTHORIZATION_REDIRECTION_LIST	String	“” (Null)	Specifies a list of IPv4, IPv6, or FQDNs of identity providers to which Avaya Vantage™ can be redirected from Avaya Aura® Device Services when USER_AUTH_FILE_SERVER_SSO is set to 3. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. Example: `SET AVAYA_AUTHORIZATION_REDIRECTION_LIST example.shibboleth.com`

SIP user-level settings

You can define the following optional device-specific parameters in the individual device-specific file settings so that the device can automatically log in to the SIP controller or server for registration and authentication. These settings must be unique across devices in order to match the settings for a SIP trunk or subscriber.

Parameter	Type	Default value	Description

Table continues…

FORCE_SIP_USERNAME	String	Null	Specifies the SIP user name that a device uses to automatically log in to the SIP controller for registration and authentication. When you set the FORCE_SIP_USERNAME, FORCE_SIP_PASSWORD, and FORCE_SIP_EXTENSION parameters for an individual device, the device does not prompt the end user to log in after it starts up. For provisioning, use the **SET** command in the individual device-specific settings file.
FORCE_SIP_PASSWORD	String	Null	Specifies the SIP password that a device uses to automatically log in to the SIP controller for registration and authentication. For provisioning, use the **SET** command in the individual device-specific settings file.
FORCE_SIP_EXTENSION	String	Null	Specifies the SIP user ID that a device uses for SIP authentication. When you set ENABLE_SIP_USER_ID to 1, configure this parameter. When ENABLE_SIP_USER_ID is set to 0, do not configure this parameter. Avaya Vantage™ uses the value in FORCE_SIP_USERNAME for both SIP authentication and SIP registration. For provisioning, use the **SET** command in the individual device-specific settings file.

Server environment settings

Define the following parameters to identify the deployment environment:

Parameter	Type	Default value	Is set to default on reset	Description
ENABLE_AVAYA_ENVIRONMENT	Numeric	1	Yes	Specifies whether the device is configured for use in an Avaya or Open SIP environment. You can assign one of the following values: • 0: The device operates in a mode to comply with a third-party SIP proxy provisioning with SIPPING-19. For the IP Office and Open SIP environments, use this value. • 1: The device operates in the Avaya environment with advanced SIP telephony features and PPM.
DISCOVER_AVAYA_ENVIRONMENT	Numeric	1	Yes	Specifies whether the device should discover and verify if the SIP controller supports Advanced SIP Telephony (AST) feature set. You can assign one of the following values: • 0: The device operates in a mode where AST features are not available. For IP Office and Open SIP environments, use this value. • 1: The device determines whether the SIP controller supports AST features in the Avaya environment. If the device receives a positive response, then it synchronizes with PPM. If the device does not receive a response, it operates in a mode where AST features are not available.
ENABLE_IPOFFICE	Numeric	0	Yes	Specifies whether the deployment environment is IP Office. You can assign one of the following values according to the deployment environment: • 0: Deployment environment other than IP Office. • 1: IP Office environment.

Network settings

The following sections describe network configuration settings, such as Ethernet, VLAN, QoS, and IEEE 802.1X.

General settings

Parameter	Type	Default value	Description
IPADD	String	0.0.0.0	Specifies the IP address of the Avaya Vantage™ device. The range is from 7 to 15 ASCII characters. This is a testable parameter. The parameter can be used in conditional statements in the `46xxsettings.txt` file. For provisioning, use: • The yiaddr field value in the DHCPACK message. • For provisioning, use the **Settings** > **Network & Internet** > **Ethernet** > **IP interface** > **Static IP settings** menu on the device.
ROUTER	String	0.0.0.0	Specifies an IP address or a list of addresses of default routers or gateways in the IP network. Entries in the list are separated by commas without any spaces between entries. The parameter can contain up to 127 characters. For provisioning, use: • The Option 3 value in a DHCPACK message. • For provisioning, use the **Settings** > **Network & Internet** > **Ethernet** > **IP interface** > **Static IP settings** menu on the device.
NETMASK	String	0.0.0.0	Specifies an IP subnet mask. This parameter specifies one IP address in the dotted decimal format. The range is from 7 to 15 ASCII characters. For provisioning, use: • The Option 1 value in a DHCPACK message. • For provisioning, use the **Settings** > **Network & Internet** > **Ethernet** > **IP interface** > **Static IP settings** menu on the device.
SUBNET	String	0.0.0.0	Specifies the subnet of the telephone. A value of SUBNET is a value of a bitwise **AND** operation performed on values of IPADD and NETMASK. The parameter can be used in conditional statements in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
USE_DHCP	Numeric	1	Specifies whether Avaya Vantage™ uses a static IP address or receives the IP address through DHCP. The options are: • 0: Use a static IP address configured on the device. • 1: Obtain the IP address automatically through DHCP. For provisioning, use the **Settings** > **Network & Internet** > **Ethernet** > **IP interface** > **Use DHCP** menu on the device.
DHCP_SSON	Numeric	242	Specifies the site-specific option number for DHCP. The range is from 128 to 254. For provisioning, use the **Settings** > **Network & Internet** > **More** > **DHCP Site Specific Option Number (SSON)** menu on the device.
DHCPSTD	Integer	0	Specifies the DHCP lease violation flag. Assign one of the following values: • 1: To comply with the DHCP standard. When the DHCP lease expires, Avaya Vantage™ immediately releases an IP address. • 0: To enter the proprietary state. When the DHCP lease expires, Avaya Vantage™ continues to use the IP address. For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.
ICMPDU	Integer	1	Specifies whether Avaya Vantage™ generates Internet Control Message Protocol (ICMP) Destination Unreachable (DU) messages to inform the source host that a port is unreachable. Assign one of the following values: • 0: DU messages are not transmitted. • 1: DU messages are only transmitted for a UDP port that ranges from 33,434 to 33,523. • 2: DU messages are transmitted. For provisioning, use: • A `name=value` pair in a DHCPACK message. • The **`SET`** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
ICMPRED	Integer	0	Specifies whether Avaya Vantage™ processes ICMP redirect messages. Assign one of the following values: • 0: Avaya Vantage™ does not process received redirect messages. • 1: Avaya Vantage™ processes received redirect messages according to RFC 1122. For provisioning, use: • A `name=value` pair in a DHCPACK message. • The **`SET`** command in the `46xxsettings.txt` file.
MTU_SIZE	Integer	1500	Specifies the Maximum Transmission Unit (MTU) size. Assign one of the following values: • 1496 • 1500 This parameter is applicable for wired Ethernet connections only and is not used for Wi-Fi. Avaya Vantage™ uses MTU_SIZE to provide compatibility with Ethernet switches that do not support the longest maximum frame length possible with tagged frames. For provisioning, use: • A `name=value` pair in a DHCPACK message. • The Option 26 value in the DHCPACK message. • The **`SET`** command in the `46xxsettings.txt` file.
NETWORK_MODE	Numeric	1	Specifies the active network interface. The available options are: • 1: Wired Ethernet connection is active. • 2: Wi-Fi connection is active. For provisioning, use the **Settings** > **Network & Internet** > **Network mode** menu on the device.
IPV6STAT	Numeric	1	Specifies the mode of the IP family to be used in the current device configuration. Assign on of the following values: • 0: Support IPv4 only mode. • 1: Support dual mode (IPv4 and IPv6). • 2: Support IPv6 only mode.

Table continues…

Parameter	Type	Default value	Description
			In an IP Office environment, set this parameter to 0 to block IPv6 traffic because Avaya Vantage™ does not support IPv6 in an IP Office environment. This parameter is applicable for both wired Ethernet and wireless connections. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.
DHCPSTDV6	Numeric	0	Specifies whether DHCPv6 will comply with the IETF RFC 8415 standard and immediately stop using an IPv6 address if the address valid lifetime expires, or whether it will enter an extended rebinding state. Assign on of the following values: • 0: If the DHCPv6 lease expires, DHCPv6 enters a proprietary extended rebinding state, in which it continues to use the IPv6 address. • 1: If the DHCPv6 lease expires, DHCPv6 complies with the IETF RFC 8415 standard and immediately releases the IPv6 address. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.
DHCPSTAT	Numeric	3	Specifies whether DHCPv4, DHCPv6, or both are to be used to assign IP addresses to the device. Assign on of the following values: • 1: Run only DHCPv4. • 2: Run only DHCPv6. • 3: Run both DHCPv4 and DHCPv6. In IPv4 only mode, if you set DHCPSTAT to 2, DHCPv4 is disabled. You cannot enable the use of DHCP through the device's **Settings** menu. Only the option for static IPv4 address configuration becomes available. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
			• The settings file received from Avaya Aura® Device Services.
PRIVACY_SLAAC_MODE	Numeric	1	Specifies the preference for privacy extensions (RFC3041) when using SLAAC to generate IPv6 addresses. Assign on of the following values: • 0: Disable privacy extensions. One stable address is generated using modified EUI-64 format interface identifier based on the device MAC address. The device address selection preference is based on default RFC6724 SASA rules. • 1: Enable privacy extensions with a preference for public addresses over temporary addresses. One stable address is generated using modified EUI-64 format interface identifier based on the device MAC address and one temporary private address is generated. This parameter value overrides the default RFC6724 SASA Rule 7 to prefer a manual, DHCPv6, or stable SLAAC address over a SLAAC temporary address. • 2: Enable privacy extensions with a preference for temporary addresses over public addresses. One stable address is generated using modified EUI-64 format interface identifier based on the device MAC address and one temporary private address is generated. The device address selection preference is based on default RFC6724 SASA rules. The default SASA rule 7 is used to prefer a SLAAC temporary address over manual, DHCPv6, or stable SLAAC addresses. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.
DUAL_IPPREF	Numeric	4	Specifies IPv4 or IPv6 preferences. The parameter controls the selection of SSON either from DHCPv4 or DHCPv6 when the device is in dual mode. DHCP clients use DUAL_IPPREF to decide which SSON configuration attributes to apply for DHCPv4 and DHCPv6 interworking in dual mode. Assign on of the following values: • 4: Prefer IPv4 over IPv6. • 6: Prefer IPv6 over IPv4.

Table continues…

Parameter	Type	Default value	Description
			For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.
SIGNALING_ADDR_MODE	Numeric	4	Specifies IPv4 or IPv6 preference for SIP registration. This parameter comes into effect only when both the device and Session Manager are in dual mode with both IPv4 and IPv6 addresses configured. Based on the value of the parameter, the Avaya™ Client SDK application uses the preferred IP addresses of Session Manager from SIP_CONTROLLER_LIST. Assign on of the following values: • 4: Prefer IPv4 over IPv6. • 6: Prefer IPv6 over IPv4. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. If Avaya Vantage™ is in IPv4 or IPv6 only mode, it ignores SIGNALING_ADDR_MODE. If Avaya Vantage™ is in IPv4 only mode, and Session Manager is either in IPv4 only or dual mode, then the SIP controller's IPv4 addresses are selected from SIP_CONTROLLER_LIST for SIP registration. If Session Manager is in IPv6 only mode, the Avaya™ Client SDK application cannot connect with the SIP controller. If Avaya Vantage™ is in IPv6 only mode, and Session Manager is either in IPv6 only or dual mode, then the SIP controller's IPv6 addresses are selected from SIP_CONTROLLER_LIST for SIP registration. **Important:** To avoid multiple registrations to the same SIP controller over IPv4 and IPv6 addresses, you must configure *only* IPv4, IPv6, or FQDN addresses for each SIP controller in SIP_CONTROLLER_LIST through all provisioning sources. Do not configure mix of IPv4 and IPv6 addresses for the same SIP controller. For provisioning, use: • The value stored on the PPM server. • The **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
			• The settings file received from Avaya Aura® Device Services. • A `name=value` pair in a DHCPACK message. • A `name=value` pair in the DHCPv6 Reply VSI option 242.
MEDIA_ADDR_MODE	Numeric	4	Specifies the preference of SDP media group lines by the active Avaya™ Client SDK application on Avaya Vantage™. If Avaya Vantage™ is in IPv4 or IPv6 only mode, it ignores MEDIA_ADDR_MODE. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. Assign on of the following values: • 4: Use IPv4. • 6: Use IPv6. • 46: Prefer IPv4 over IPv6. • 64: Prefer IPv6 over IPv4. For provisioning, use: • The value stored on the PPM server. • The **`SET`** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. • A `name=value` pair in a DHCPACK message. • A `name=value` pair in the DHCPv6 Reply VSI option 242.
IPV6DADXMITS	Numeric	1	Specifies whether Duplicate Address Detection (DAD) is performed on tentative addresses, as specified in RFC 4862. A non-zero value specifies the maximum number of transmitted Neighbor Solicitation (NS) messages to determine whether an IPv6 address is already in use. The value can be in the range from 0 to 5. Assign on of the following values: • 0: Disable DAD. • 1 to 5: Enable DAD. The value indicates the maximum number of transmitted NS messages.

Table continues…

Parameter	Type	Default value	Description
			For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.
BLUETOOTHSTAT	Numeric	1	Specifies whether Bluetooth is allowed for user configuration. Assign one of the following values: • 0: Bluetooth and the **Bluetooth** menu are disabled in the **Settings** menu on the device. The user cannot enable Bluetooth. • 1: Bluetooth and the **Bleutooth** menu are enabled in the **Settings** menu on the device. The user can enable or disable Bluetooth. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
BLUETOOTH_FEATURES_SHARED_VIA_STAT	Numeric	0	Specifies whether users have access to **Shared via Bluetooth** options in the **Setting** menu on the device. • 0: Users cannot use **Shared via Bluetooth**. • 1: Users can use **Shared via Bluetooth**. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
TRUST_AGENTS_STAT	Numeric	1	Specifies whether users can configure trust agents. • 0: Users cannot access **Trust agents** in the **Settings** menu. All trust agents are disabled. • 1: Users can access **Trust agents** in the **Settings** menu. Users can enable or disable the available trust agents For provisioning, use the **SET** command in the `46xxsettings.txt` file.
TRUST_AGENTS_SMARTLOCK_STAT	Numeric	1	Specifies whether users can configure the Google Smart Lock feature. • 0: Users cannot access **Smart Lock** in the **Settings** menu. Smart Lock (Google) is disabled. • 1: Users can access **Smart Lock** in the **Settings** menu. Users can enable or disable the Smart Lock (Google) feature. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
TRUST_AGENTS_AVAYA_SMARTLOCK_STAT	Numeric	1	Specifies whether users can configure the Avaya Smart Lock feature. • 0: Users cannot access **Avaya Smart Lock** in the **Settings** menu. The Avaya Smart Lock feature is disabled. • 1: Users can access **Avaya Smart Lock** in the **Settings** menu. Users can enable or disable the Avaya Smart Lock feature. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
WIFISTAT	Numeric	1	Specifies whether users can configure Wi-Fi. • 0: Wi-Fi is disabled. Users cannot enable Wi-Fi. • 1: Wi-Fi is enabled. Users can configure Wi-Fi settings through the device **Settings** menu on the device. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
WIFIAPSTAT	Numeric	0	Specifies whether users can configure the WI-FI access point. • 0: WI-FI access point is disabled. Users cannot enable the access point. • 1: Users can enable and configure the access point. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
WIFI_CON_STATUS_ON_LOGOUT	Numeric	1	Specifies whether Avaya Vantage™ keeps information about wireless connections after logout. • 0: Avaya Vantage™ deletes information about Wi-Fi connections, such as Wi-Fi passwords. • 1: Avaya Vantage™ keeps information about Wi-Fi connections and the active wireless connection, such as Wi-Fi passwords. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
GRATARP	Numeric	0	Specifies whether an existing Address Resolution Protocol (ARP) cache entry is updated with a MAC

Table continues…

Parameter	Type	Default value	Description
			address received in a gratuitous ARP message. Assign one of the following values: • 0: Avaya Vantage™ ignores gratuitous ARP messages. • 1: Avaya Vantage™ uses gratuitous ARP messages to update the existing ARP cache entry. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Ethernet interface settings

Parameter	Type	Default value	Is set to default on reset	Description
PHY1STAT	Numeric	1	Yes	Specifies the speed and duplex settings for the primary Ethernet line interface. Assign one of the following values: • 1: Speed and duplex are auto negotiated. Use the auto negotiation setting when the connected network switch is also configured for auto negotiation. • 5: 100 Mbps full-duplex operation is supported. Use this setting when the connected network switch is also configured for 100 Mbps full-duplex mode. For provisioning, use: • A `name=value` pair in a DHCPACK message. • DHCP option 43. • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. • The **Settings** > **Network & Internet** > **Ethernet** > **Interfaces** > **Ethernet** menu on the device.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
PHY2STAT	Numeric	1	Yes	Disables the secondary Ethernet line interface or specifies its speed and duplex settings. Assign one of the following values: • 0: The secondary Ethernet interface is disabled. • 1: Speed and duplex are auto negotiated. Use the auto negotiation setting when the connected network device is also configured for auto negotiation. • 5: 100 Mbps full-duplex operation is supported. Use this setting when the connected network device is configured for 100 Mbps full-duplex mode. For provisioning, use: • A `name=value` pair in a DHCPACK message. • DHCP option 43. • The **`SET`** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. • The **Settings** > **Network & Internet** > **Ethernet** > **Interfaces** > **PC Ethernet** menu on the device.
PHY2_AUTOMDIX_ENABLED	Numeric	1		Specifies whether auto-MDIX is enabled on the secondary Ethernet port. Assign one of the following values: • 0: Auto-MDIX is disabled. • 1: Auto-MDIX is enabled. For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.
PORT_MIRRORING	Numeric	0		Specifies whether Ethernet packets transmitted or received on the primary Ethernet port are copied to the secondary Ethernet port. Assign one of the following values: • 0: Disabled. • 1: Enabled. For provisioning, use the **Settings** > **Debugging options** > **Port mirroring** menu on the device.

VLAN settings

Parameter	Type	Default value	Is set to default on reset	Description
L2Q	Numeric	0	Yes	Specifies 802.1Q tagging mode. Assign one of the following values: • 0: Auto • 1: On • 2: Off For provisioning, use: • A `name=value` pair in a DHCPACK message. The precedence is 1. • DHCP option 43. The precedence is 1. • The **`SET`** command in the `46xxsettings.txt` file. The precedence is 3. • LLDP. The precedence is 4. - The Avaya/Extreme Proprietary 802.1Q Framing TLV. - The parameter is set indirectly by receiving a VLAN name with the “voice” prefix in the IEEE 802.1 VLAN Name TLV. - The T flag in the TIA LLDP MED Network policy TLV. • The **Settings** > **Network & Internet** > **Ethernet** > **VLAN** > **VLAN tagging (802.1Q)** menu on the device. The precedence is 5.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
L2QVLAN	Numeric	0	Yes	Specifies the 802.1Q VLAN identifier. The range is from 0 to 4094. This parameter is initialized from L2QVLAN_INIT after turning the device on. The parameter is not initialized from L2QVLAN_INIT after reset. For provisioning, use: • A `name=value` pair in a DHCPACK message. The precedence is 1. • DHCP option 43. The precedence is 1. • The **`SET`** command in the `46xxsettings.txt` file. The precedence is 3. • LLDP. The precedence is 4. - The parameter is set indirectly by receiving a VLAN name with the “voice” prefix in the IEEE 802.1 VLAN Name TLV. - The TIA LLDP MED Network policy TLV. The **Settings** > **Network & Internet** > **Ethernet** > **VLAN** > **VLAN** menu on the device. The precedence is 5.
VLANTEST	Numeric	60	Yes	Specifies the number of seconds that Avaya Vantage™ waits for DHCPOFFER message reception on a non-zero VLAN. The range is from 0 to 999. For provisioning, use: • A `name=value` pair in a DHCPACK message. • The **`SET`** command in the `46xxsettings.txt` file. • The **Settings** > **Network & Internet** > **Ethernet** > **VLAN** > **VLAN test timer** menu on the device.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
PHY2TAGS	Numeric	0		Controls whether VLAN tags are stripped from frames forwarded to the secondary Ethernet interface. Assign one of the following values: • 0: VLAN tags are removed from frames forwarded to the secondary Ethernet interface. 1: VLAN tags are not removed from frames forwarded to the secondary Ethernet interface. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
PHY2VLAN	Numeric	0		Specifies the value of the 802.1Q VLAN identifier that is used to identify tagged frames through the secondary Ethernet interface. Valid values are 0 through 4094. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. The precedence is 3. • LLDP. The precedence is 4.
VLANSEP	Numeric	1		Specifies whether the VLAN separation is enabled or disabled. Assign one of the following values: • 0: Disabled. • 1: Enabled. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Note:

The parameters VLANSEP, PHY2TAGS, PHY2VLAN, DOT1X, PHY2_AUTOMDIX_ENABLED, and PHY2STAT are supported by K165 and K175 devices that have an embedded Ethernet switch.

All K155 devices have an embedded Ethernet switch.

IEEE 802.1X settings

Parameter	Type	Default value	Is set to default on reset	Description
DOT1X	Numeric	0	Yes	Specifies whether the IEEE 802.1X Pass through operating mode is enabled on Avaya Vantage™. Pass through is the forwarding of Extensible Authentication Protocol over LAN (EAPOL) frames between the device's Ethernet line interface and its secondary (PC) Ethernet interface. The options are: • 0: EAPOL multicast pass-through is enabled without proxy logoff. • 1: EAPOL multicast pass-through is enabled with proxy logoff. • 2: EAPOL multicast pass-through is disabled. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** > **Network & Internet** > **Ethernet** > **IEEE 802.1x authentication** > **Pass through mode** menu on the device.
DOT1XSTAT	Numeric	0	Yes	Specifies whether the IEEE 802.1X supplicant operating mode for Ethernet is enabled on Avaya Vantage™. The options are: • 0: Supplicant operation is disabled. • 1: Supplicant operation is enabled. Avaya Vantage™ responds only to received unicast Extensible Authentication Protocol over LAN (EAPOL) messages. • 2: Supplicant operation is enabled. Avaya Vantage™ responds to received unicast and multicast EAPOL messages. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** > **Network & Internet** > **Ethernet** > **IEEE 802.1x authentication** > **Supplicant mode** menu on the device.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
DOT1XEAPS	String	MD5	Yes	Specifies a list of Extensible Authentication Protocol (EAP) methods for IEEE 802.1x authentication. Assign one of the following values: • TLS • MD5 The range is a default string length. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** > **Network & Internet** > **Ethernet** > **IEEE 802.1x authentication** > **EAP Type** menu on the device.
DOT1XID	String	Ethernet MAC Address of the device ($MACADDR) without the colon separators	Yes	Specifies the IEEE 802.1X Supplicant identifier for the Ethernet option. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** > **Network & Internet** > **Ethernet** > **IEEE 802.1x authentication** > **802.1x credentials** menu on the device.
DOT1XPSWD	String	Null	Yes	Specifies the IEEE 802.1X password for the Ethernet option. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** > **Network & Internet** > **Ethernet** > **IEEE 802.1x authentication** > **802.1x credentials** menu on the device.

Active phone application

Parameter	Type	Default value	Is set to default on reset	Description
ACTIVE_CSDK_BASED_PHONE_APP	String	null string	Yes	The package name of an active CSDK-based phone application. Only one CSDK-based application can be active at a time. When the parameter is set to the default value, Avaya Vantage™ operates in the non Avaya™ Client SDK application based mode. In this case, the Login screen and configuration sharing are not supported. Some configuration parameters are also not supported. **Important:** The ACTIVE_CSDK_BASED_PHONE_APP must only be used when the active phone application is an Avaya™ Client SDK application. Otherwise, this parameter must use the default value. For provisioning, use the **SET** command in the `46xxsettings.txt` file. With IP Office, this parameter is automatically-generated and is present in the `K1xxSupgrade.txt` file.

Application settings

Parameter	Type	Default value	Is set to default on reset	Description
PUSH_APPLICATION	String	null string	Yes	Specifies a list of applications that administrators define for installation on Avaya Vantage™. Each entry in the list represents a URL of the application. The URL can be specified using: • The relative path format. The origin is the directory specified by the FILE_SERVER_URL or HTTPDIR and TLSDIR parameters depending on whether the download uses HTTP or HTTPS. • The absolute path format. In this case, the URL must begin with `http://` or `https://`. Each entry of the list must be separated by commas without any spaces between entries. Each entry consists of an application's display name followed by an equal sign (=) and a file name or URL. If display names contain space characters, you must enclose the list using double quotes. For provisioning, use the **SET** command in the `46xxsettings.txt` file. With IP Office, this parameter is automatically-generated and is present in the `K1xxSupgrade.txt` file.
APPS_CONTROL_FILE	String	null string	Yes	Specifies a path to a file containing third-party applications installation rules for end users (black and white lists). The path is represented by a URL. The URL can be specified using: • Relative path format. Origin is the directory specified by the FILE_SERVER_URL or HTTPDIR and TLSDIR parameters depending on whether the download uses HTTP or HTTPS • Absolute path format. In this case, the URL must begin with `http://` or `https://` For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
USER_INSTALL_APPS_GOOGLE_PLAY_STORE	Numeric	1	Yes	Specifies whether end users can install applications from Google Play. Assign one of the following values: • 0: End users cannot install applications. • 1: End users can install applications. For provisioning, use the **SET** command in the `46xxsettings.txt` file. With IP Office, configure this parameter in the `46xxspecials.txt` file.

PIN_APP	String	null string	Yes	Specifies the package name of the application that must be pinned after a device restart. If this parameter is configured and the specified application is installed, Avaya Vantage™ shows this application after login. Users cannot switch to another application or navigate to the device Home screen.
				You can also specify a comma-separated list of package names for applications to be pinned using an Avaya Launcher for Kiosk mode. You must push the launcher onto the device using the PUSH_APPLICATION parameter. In the PIN_APP value, you can specify up to six Android applications to be displayed in Kiosk mode.
				For provisioning, use the **SET** command in the `46xxsettings.txt` file.
				Example of pinning only one application, Avaya Vantage™ Connect:
				`SET PIN_APP "com.avaya.android.vantage.basic"`
				Example of using the Avaya Launcher application, “com.avaya.endpoint.avayakiosk”, for Kiosk mode:
				`SET PIN_APP "com.avaya.android.vantage.basic,com.avaya.endpoint.avayakiosk,com.avaya.endpoint.login,com.android.chrome"`
				In the above example, the pinned applications are Avaya Vantage™ Connect and Chrome. The login package, “com.avaya.endpoint.login”, makes the lock and logout options available in Kiosk mode.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
USER_INSTALL_APPS_UNKNOWN_SOURCES	Numeric	1	Yes	Specifies whether third-party applications from unknown, non-Google Play sources can be installed on Avaya Vantage™. Assign one of the following values: • 0: Installation of third-party applications from unknown sources is disabled. End users cannot change the status through the **Settings** menu on the device. • 1: Installation of third-party applications from unknown sources is disabled by default. End users can change the status through the **Settings** menu. • 2: Installation of third-party applications from unknown sources is enabled by default. End users can change the status through the **Settings** menu. When installation of applications from unknown sources is enabled, end users can download application APKs from non-Google Play sources, such as common third-party application stores, emails, and websites. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Avaya™ Client SDK application parameters

The following parameters are supported by Avaya™ Client SDK applications, including Avaya Vantage™ Connect and Avaya IX™ Workplace Client, on Avaya Vantage™.

For additional parameters specific to Avaya Vantage™ Connect, see Avaya Vantage Connect parameters on page 261.

For a detailed list of parameters supported by Avaya IX™ Workplace Client on Avaya Vantage™, see *Planning for and Administering Avaya IX™ Workplace Client for Android, iOS, Mac, and Windows*.

Avaya Aura® Device Services parameters

Parameter	Type	Default value	Description
ACSENABLED	Numeric	0	Specifies whether the CSDK-based telephony application uses contacts stored on Avaya Aura® Device Services. You can assign one of the following values: • 0: The application does not use contacts from Avaya Aura® Device Services. Instead, it uses PPM contacts. • 1: The application uses contacts from Avaya Aura® Device Services. The application does not use PPM contacts. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ACSSRVR	String	Null string	Specifies the address of Avaya Aura® Device Services contact services. The address is either an IP address in the dotted decimal format or a domain name. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ACSPORT	Numeric	443	Specifies the port number the CSDK-based telephony application uses to connect to Avaya Aura® Device Services contact services. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ACSSECURE	Numeric	1	Specifies whether a secure connection is used. Assign one of the following values: • 0: Secure connection is not used. The application uses HTTP over TCP. • 1: Secure connection is used. The application uses HTTPS over TLS. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
ACSSSO	Numeric	1	Specifies whether the Avaya™ Client SDK application uses unified login credentials to access Avaya Aura® Device Services. Assign one of the following values: • 0: Use of unified login credentials to log in to Avaya Aura® Device Services automatically is disabled. You must enter the Avaya Aura® Device Services credentials manually on the application. • 1: Use of unified login credentials is enabled. If you log in to Avaya Vantage™ with these credentials, the application is connected with Avaya Aura® Device Services automatically. Only Avaya IX™ Workplace Client supports configuration of this parameter. Avaya Vantage™ Connect only supports 1 as the ACSSSO parameter value. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Layer 2 QoS parameters

Important:

The Avaya™ Client SDK application does *not* use the following parameter values received from PPM in an Avaya Aura® environment. Instead, the application uses the values that Avaya Vantage™ collects from other provisioning sources as mentioned in the parameter description in the table.

Parameter	Type	Default value	Description
L2QAUD	Numeric	6	Specifies the layer 2 priority value for audio frames generated by the Avaya™ Client SDK application. You can assign a value from 0 to 7. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. The precedence is 3. • The settings file received from Avaya Aura® Device Services. The precedence is 4. • The TIA LLDP MED Network policy TLV. The precedence is 5.

Table continues…

Parameter	Type	Default value	Description
L2QVID	Numeric	5	Specifies the layer 2 priority value for video frames generated by the Avaya™ Client SDK application. You can assign a value from 0 to 7. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. The precedence is 3. • The settings file received from Avaya Aura® Device Services. The precedence is 4. • The TIA LLDP MED Network policy TLV. The precedence is 5.
L2QSIG	Numeric	6	Specifies the layer 2 priority value for signaling frames generated by the Avaya™ Client SDK application. You can assign a value from 0 to 7. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. The precedence is 3. • The settings file received from Avaya Aura® Device Services. The precedence is 4. • The TIA LLDP MED Network policy TLV. The precedence is 5.

Layer 3 QoS parameters

Important:

Since Avaya™ Client SDK Release 4.4, an Avaya™ Client SDK application no longer uses the following parameter values received from PPM in an Avaya Aura® environment. Instead, the application uses the values that Avaya Vantage™ collects from other provisioning sources as mentioned in the parameter descriptions in the table.

Parameter	Type	Default value	Description
DSCPAUD	Numeric	46	Specifies the decimal presentation of Differentiated Services Code Point (DSCP) for audio frames generated by the device. You can assign a value from 0 to 63. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. The precedence is 3. • The settings file received from Avaya Aura® Device Services. The precedence is 4. • The TIA LLDP MED Network policy TLV. The precedence is 5.
DSCPSIG	Numeric	34	Specifies the decimal presentation of DSCP for signaling frames generated by the device. You can assign a value from 0 to 63. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. The precedence is 3. • The settings file received from Avaya Aura® Device Services. The precedence is 4. • The TIA LLDP MED Network policy TLV. The precedence is 5.
DSCPVID	Numeric	34	Specifies the decimal presentation of DSCP for video frames generated by the device. You can assign a value from 0 to 63. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. The precedence is 3. • The settings file received from Avaya Aura® Device Services. The precedence is 4. • The TIA LLDP MED Network policy TLV. The precedence is 5.

RTP parameters

Parameter	Type	Default value	Description
RTP_PORT_LOW	Numeric	5004	Specifies the minimum UDP port range value to be used by RTP/RTCP or SRTP/SRTCP connections. You can assign a value between 1024 and 65503. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
RTP_PORT_RANGE	Numeric	40	Specifies the UDP port range that Avaya Vantage™ Connect uses for RTP/RTCP or SRTP/SRTCP connections. You can assign a value between 32 and 64511. The maximum value of the range is calculated as a sum of the RTP_PORT_LOW and RTP_PORT_RANGE values. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

SRTP parameters

Parameter	Type	Default value	Description
MEDIAENCRYPTION	String	1,2,9	Specifies which media encryption options are supported. The value of the parameter is a list of up to 3 options, which must be separated by commas. The following options are available: • 1: aescm128–hmac80 • 2: aescm128–hmac32 • 9: none • 10: aescm256–hmac80 • 11: aescm256–hmac32 For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ENCRYPT_SRTCP	Numeric	0	Specifies whether RTCP packets are encrypted. SRTCP is only used if encryption is enabled using MEDIAENCRYPTION. Assign one of the following values: • 0: SRTCP is disabled. • 1: SRTCP is enabled. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Audio codec parameters

Parameter	Type	Default value	Description
ENABLE_OPUS	Numeric	1	Specifies whether the OPUS codec is enabled. Assign one of the following values: • 0: Disabled. • 1: Enabled WIDEBAND_20K. • 2: Enabled NARROWBAND_16K. • 3: Enabled NARRWOBAND_12K. For Avaya Vantage™ Connect, this parameter is supported in both the Avaya Aura® and IP Office environments. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
OPUS_PAYLOAD_TYPE	Numeric	116	Specifies the RTP payload type that is used for the OPUS codec. The range is from 96 to 127. This parameter is used when media offer is sent to the far end in **INVITE** or 200 OK when **INVITE** with no SDP is received. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Audio parameters

Parameter	Type	Default value	Description
AUDIO_DEVICE_CALL_CONTROL_ENABLED	Numeric	1	Specifies whether Avaya IX™ Workplace Client on Avaya Vantage™ supports call control through headset and speakerphone buttons. This parameter is not applicable for Avaya Vantage™ Connect. You cannot disable call control through headsets and speakerphones on Avaya Vantage™ Connect. USB headsets support answer, end, and mute call operations. Bluetooth headsets support answer and end call operations. You can assign one of the following values: • 0: Call control through headset and speakerphone buttons is disabled. • 1: Call control through headset and speakerphone buttons is enabled. Avaya IX™ Workplace Client Release 3.7.1 and later support this parameter. As of Avaya IX™ Workplace Client Release 3.7.4, the default parameter value is 1. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Video parameters

Parameter	Type	Default value	Description
VIDEO_MAX_BANDWIDTH_ANY_NETWORK	Numeric	1280	Specifies the maximum bandwidth for video calls. The bandwidth is measured in kilobits per second (kbps). You can assign one of the following values: • 0: Video is blocked. • 1 to 10000: Maximum allowed bandwidth. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ENABLE_VIDEO	Numeric	1	Specifies whether video is enabled or disabled. You can assign one of the following values: • 0: Video is disabled. • 1: Video is enabled. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Logging parameters

Parameter	Type	Default value	Description
LOG_VERBOSITY	Numeric	0	Specifies whether verbose logging is enabled. Assign one of the following values: • 0: Only Info log messages are collected. • 1: Debug and Info log messages are collected. Use this value to collect logs for debugging purposes. If the parameter value is changed, changes will be applied after reboot. **Note:** To collect application logs, you must also enable logging and set up the local and remote logging level on Avaya Vantage™. Assign one of the following values to the SYSLOG_LEVEL and LOCAL_LOG_LEVEL parameters: • Debug: To collect Debug log messages. • Notice: To collect Info log messages.
ANALYTICSENABLED	Integer	1	Defines whether to allow Avaya to collect data using Google Analytics on behalf of the administrator's user community. Assign one of the following values: • 0: Data collection is disabled. • 1: Data collection is enabled. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
SUPPORTEMAIL	String	Null	Defines the default email address for sending diagnostic logs. The parameter value is used when you try to send the debug or audio report to an email application. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Contact parameters

Parameter	Type	Default value	Description
NAME_SORT_ORDER	String	last,first	Specifies how contact names are sorted by the active Avaya™ Client SDK application. You can assign one of the following values: • last,first: The active Client SDK application sorts contacts according to the last name and then the first name. • first,last: The active Client SDK application sorts contacts according to the first name and then the last name. For example: `SET NAME_SORT_ORDER "first,last"`. For provisioning, use the **SET** command in the `46xxsettings.txt` file. You can also set this parameter value using the settings menu option on the Client SDK application.
NAME_DISPLAY_ORDER	Numeric	0	Specifies how contact names are displayed by the active Avaya™ Client SDK application. You can assign one of the following values: • 0: The active Client SDK application displays the last name followed by the first name. • 1: The active Client SDK application displays the first name followed by the last name. For provisioning, use the **SET** command in the `46xxsettings.txt` file. You can also set this parameter value using the settings menu option on the Client SDK application.

Dialing rule parameters

Parameter	Type	Default value	Description
ENHDIALSTAT	Numeric	1	Specifies whether the dialing rules are used during certain dialing activities. Assign one of the following values: • 0: To disable the dialing algorithm. • 1: To enable the dialing algorithm for all outgoing calls.
PHNCC	String	Null string	Specifies the country code. Valid values are from 1 to 999.

Table continues…

Parameter	Type	Default value	Description
PHNIC	String	Null string	Specifies the access code that you dial to make international calls. The value can be of 0 to 4 characters in length. The allowed characters are 0-9, *, and #.
PHNLD	String	Null string	Specifies the access code that you dial to make long distance calls. Valid values are from 0 to 9, and null string (“”). If long distance access code is not required, set the value to “”
PHNDPLENGTH	String	Null string	Specifies the length of internal extension numbers. The value must match the extension length set on the call server. The valid range is from 3 to 13.
PHNLDLENGTH	String	Null string	Specifies the length of national phone numbers of the country that is considered in the dial plan. Valid values are from 5 to 15.
PHNOL	String	Null string	Specifies the outside line access code, which is the number you press to access an external line. The value can be of 0 to 2 characters in length. The allowed characters are 0-9, *, and #.
APPLY_DIALINGRULES_TO_PLUS_NUMBERS	Numeric	0	Specifies whether to apply dialing rules on phone numbers with the plus sign (+) at the beginning. Assign one of the following values: • 0: To ignore the dialing rules for phone numbers that begin with the plus sign (+). • 1: To replace the plus sign (+) with dial plan digits. In Avaya Aura®, whenever possible, configure the plus (+) dialing option in Session Manager instead of enabling this parameter.
AUTOAPPLY_ARS_TO_SHORTNUMBERS	Numeric	1	Specifies whether to disable the dialing rules logic that automatically appends the outside line access code (PHNOL) to numbers that are shorter than the shortest extension length. Assign one of the following values: • 0: To disable the logic. The PHNOL code is not appended to numbers that are shorter than the shortest extension length. • 1: To enable the logic. The PHNOL code is appended to numbers that are shorter than the shortest extension length.

Table continues…

Parameter	Type	Default value	Description
PHNREMOVEAREACODE	String	0	Specifies whether the area code must be removed for local calls. This parameter is obsolete. While it is still supported for backward compatibility, Avaya recommends that you use the newer parameter, DIALPLANLOCALCALLPREFIX.
DIALPLANLOCALCALLPREFIX	String	0	Indicates whether the area code must be removed for local calls. Assign one of the following values: • 0: To disable the removal of the area code for local calls. • 1: To enable the removal of the area code for local calls. **Note:** The area code is configured using DIALPLANAREACODE.
DIALPLANNATIONALPHONENUMLENGTHLIST	String	Null string	Specifies a list of national phone number length (PHNLDLENGTH) values separated by commas. This parameter takes precedence over PHNLDLENGTH. Example: `SET DIALPLANNATIONALPHONENUMLENGTHLIST 10,11`
DIALPLANEXTENSIONLENGTHLIST	String	Null string	Specifies a list of internal extension length (PHNDPLENGTH) values separated by commas. This parameter takes precedence over PHNDPLENGTH. Example: `SET DIALPLANEXTENSIONLENGTHLIST 7,8`
DIALPLANPBXPREFIX	String	Null string	Specifies the PBX main prefix.
PHNPBXMAINPREFIX	String	Null string	Specifies the PBX main prefix. This parameter is obsolete. While it is still supported for backward compatibility, Avaya recommends that you use the newer parameter, DIALPLANPBXPREFIX.
DIALPLANAREACODE	String	Null string	Specifies the area or city code.
SP_AC	String	Null string	Specifies the area or city code. This parameter is obsolete. While it is still supported for backward compatibility, Avaya recommends that you use the newer parameter, DIALPLANAREACODE.

Conferencing parameters

Parameter	Type	Default value	Description
CONFERENCE_FACTORY_URI	String	Null string	Specifies the URI for network conferencing in an IP Office deployment. The URI consists of a dial string followed by @, followed by a domain. Example: `SET CONFERENCE_FACTORY_URI "93375000@avaya.com"` With IP Office, this parameter is automatically generated.

Audio and video preferences settings for meetings

Parameter	Type	Default value	Description
PREF_MUTE_MIC_WHEN_JOINING_MEETING	Numeric	1	Specifies whether microphone is muted when joining meetings through Avaya Vantage™ Connect or Avaya IX™ Workplace Client. You can assign one of the following values: • 0: Not to mute the microphone when joining a meeting. • 1: To mute the microphone when joining a meeting. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
PREF_BLOCK_CAMERA_WHEN_JOINING_MEETING	Numeric	1	Specifies whether the camera is blocked when joining meetings through Avaya Vantage™ Connect or Avaya IX™ Workplace Client. You can assign one of the following values: • 0: Not to block the camera when joining a meeting. • 1: To block the camera when joining a meeting. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Exchange Web Services (EWS) settings

Parameter	Type	Default value	Description
EWSENABLED	Numeric	0	Specifies whether EWS is enabled. The Avaya™ Client SDK application can access Microsoft Exchange Calendar information only when EWS is enabled. You can assign one of the following values: • 0: To disable EWS. • 1: to enable EWS. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
EWSSERVERADDRESS	String	Null string	Specifies the server address that can be used to connect to EWS directly. If you configure this parameter, the application tries to establish a connection to EWS directly using the server address and avoids the auto discovery process. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
EWSDOMAIN			Specifies the Microsoft Exchange server domain to which Avaya™ Client SDK must register. Avaya™ Client SDK uses this parameter for auto discovery of the domain if the domain is not part of the Microsoft Exchange or unified login user name. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
EWSSSO	Numeric	1	Specifies whether the Avaya™ Client SDK application uses dedicated login credentials or unified login credentials to connect to the Microsoft Exchange server. You can assign one of the following values: • 0: To disable the use of unified login credentials. You must enter the Microsoft Exchange user credentials manually on the application to view calendar information. • 1: To enable the use of unified login credentials. If you log in to Avaya Vantage™ using unified login credentials, the application is connected with the Microsoft Exchange Calendar service automatically. • 4: To enable the use of Microsoft Modern authentication. You can enter your Exchange Calendar credentials on the Microsoft Modern authentication web page. Currently, only Avaya IX™ Workplace Client supports this value. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Services SSO settings

Parameter	Type	Default value	Description
ESMSSO	Numeric	1	Specifies whether the Messaging service uses unified login credentials. Only Avaya IX™ Workplace Client supports this parameter on Avaya Vantage™. Assign one of the following values: • 0: Use of unified login credentials for the Messaging service is disabled. You must enter the Messaging credentials manually on the application. • 1: Use of unified login credentials is enabled. If you log in to Avaya Vantage™ with these credentials, the application is connected to the Messaging service automatically. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
UNIFIED_PORTAL_SSO	Numeric	1	Specifies whether Unified Portal uses unified login credentials on Avaya IX™ Workplace Client. Only Avaya IX™ Workplace Client supports this parameter on Avaya Vantage™. Assign one of the following values: • 0: Use of unified login credentials for Unified Portal is disabled. You must enter the Unified Portal credentials manually on the application. • 1: Use of unified login credentials is enabled. If you log in to Avaya Vantage™ with these credentials, the application is connected to the Unified Portal service automatically. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Avaya Vantage™ Connect parameters

Use the following parameters to customize Avaya Vantage™ Connect on Avaya Vantage™.

Call option parameters

Parameter	Type	Default value	Description
ENABLE_REDIAL	Numeric	1	Specifies whether the **Redial** button is available to users. You can assign one of the following values: • 0: The **Redial** button is unavailable. • 1: The **Redial** button is available. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
CCBTNSTAT	Numeric	1	Specifies whether you can enable or disable the conferencing, call transfer, call hold, and mute features separately using the corresponding parameters. You can assign one of the following values: • 0: Avaya Vantage™ Connect uses the values of parameters related to these features. You can configure the availability of each feature separately. • 1: Avaya Vantage™ Connect ignores the values of parameters related to these features. All features are available to users. When CCBTNSTAT is set to 0, use the following parameters to configure feature availability: • CONFSTAT: For conferencing • HOLDSTAT: For call hold • MUTESTAT: For mute • XFERSTAT: For call transfer For provisioning, use the **SET** command in the `46xxsettings.txt` file.
HOLDSTAT	Numeric	1	Specifies whether the **Hold** button is available to users. Avaya Vantage™ Connect ignores this parameter if CCBTNSTAT is set to 1. Assign one of the following values: • 0: The **Hold** button is disabled. • 1: The **Hold** button is enabled. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
MUTESTAT	Numeric	1	Specifies whether the **Mute** button is available to users. This option controls muting for both audio and video. Avaya Vantage™ Connect ignores this parameter if CCBTNSTAT is set to 1. You can assign one of the following values: • 0: The **Mute** button is disabled. • 1: The **Mute** button is enabled. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
CONFSTAT	Numeric	1	Specifies whether the **Conference** button is available to users. Avaya Vantage™ Connect ignores this parameter if CCBTNSTAT is set to 1. You can assign one of the following values: • 0: The **Conference** button is disabled. • 1: The **Conference** button is enabled. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
XFERSTAT	Numeric	1	Specifies whether the **Call transfer** button is available to users. Avaya Vantage™ Connect ignores this parameter if CCBTNSTAT is set to 1. You can assign one of the following values: • 0: The **Call transfer** button is disabled. • 1: The **Call transfer** button is enabled. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
POUND_KEY_AS_CALL_TRIGGER	Numeric	1	In off-hook dialing, specifies whether: • Pressing the pound key (#) triggers a call. • The pound key is considered a dialed digit. You can assign one of the following values: • 0: The pound key is considered a dialed digit. • 1: The pound key triggers a call. In the IP Office environment, set POUND_KEY_AS_CALL_TRIGGER to 0. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ENABLE_JOIN_EQUINOX_MEETING	Numeric	1	Specifies whether the **Join Equinox Meeting** icon is available in the Dial pad tab on Avaya Vantage™ Connect. You can assign one of the following values: • 0: The **Join Equinox Meeting** icon is unavailable. • 1: The **Join Equinox Meeting** icon is available. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Audio codec parameters

Parameter	Type	Default value	Description
ENABLE_G711A	Numeric	1	Specifies whether the G.711 a-law codec is enabled. You can assign one of the following values: • 0: Disabled. • 1: Enabled. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ENABLE_G711U	Numeric	1	Specifies whether the G.711 mu-law codec is enabled. You can assign one of the following values: • 0: Disabled. • 1: Enabled. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ENABLE_G722	Numeric	1	Specifies whether the G.722 codec is enabled. You can assign one of the following values: • 0: Disabled. • 1: Enabled. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ENABLE_G726	Numeric	1	Specifies whether the G.726 codec is enabled. You can assign one of the following values: • 0: Disabled. • 1: Enabled. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ENABLE_G729	Numeric	1	Specifies whether the G.729A codec is enabled. You can assign one of the following values: • 0: Disabled. • 1: Enabled without Annex B support. • 2: Enabled with Annex B support. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Audio parameters

Parameter	Type	Default value	Description
ADMIN_CHOICE_RINGTONE	String	Default	Specifies the ring tone that Avaya Vantage™ Connect uses for incoming calls. When the parameter is set to “Default”, the Avaya built-in ringtone is used for incoming calls. Otherwise, you can specify the name of one of the ringtones available on the device. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Contact parameters

Parameter	Type	Default value	Description
ENABLE_CONTACTS	Numeric	1	Specifies whether the Contacts tab is available on Avaya Vantage™ Connect. You can assign one of the following values: • 0: The Contacts tab is unavailable. • 1: The Contacts tab is available on the application. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ENABLE_MODIFY_CONTACTS	Numeric	1	Specifies whether users can modify contacts. You can assign one of the following values: • 0: Users cannot modify contacts. • 1: Users can modify contacts. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ENABLE_FAVORITES	Numeric	1	Specifies whether the Favorites tab is available on Avaya Vantage™ Connect. You can assign one of the following values: • 0: The Favorites tab is unavailable. • 1: The Favorites tab is available on the application. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Call log parameter

Parameter	Type	Default value	Description
ENABLE_CALL_LOG	Numeric	1	Specifies whether the Call History tab is available on Avaya Vantage™ Connect. You can assign one of the following values: • 0: The Call History tab is unavailable. • 1: The Call History tab is available on the application. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Calendar parameter

Parameter	Type	Default value	Description
ENABLE_CALENDAR	Numeric	0	Specifies whether the Calendar tab is available on Avaya Vantage™ Connect. You can assign one of the following values: • 0: The Calendar tab is unavailable. • 1: The Calendar tab is available. For provisioning, use the **SET** command in the `46xxsettings.txt` file. The device user can also enable or disable the Calendar tab through the Avaya Vantage™ Connect application settings.

Application logo and icon display parameters

Parameter	Type	Default value	Description
BRANDING_FILE	String	Null (“”)	Specifies the URL to download a branding logo image. Avaya Vantage™ Connect displays this image on the top left corner of all screens instead of the Avaya logo. Specify the URL using the absolute path format, where the URL must start with either `http://` or `https://`. The image must be of the following settings: • Resolution: 142x56. • File format: PNG, JPG (JPEG), GIF, or BMP. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
COMPANION_APPLICATION	String	Null (“”)	Specifies the Android package name of the companion application to be used with Avaya Vantage™ Connect application running on the same Avaya Vantage™ device. When you keep the default value, then Avaya Vantage™ Connect displays only the branding logo, which is defined in BRANDING_FILE, on its top left corner. When you configure COMPANION_APPLICATION with the Android package name of the companion application installed on the device, Avaya Vantage™ Connect displays an additional icon, which represents the companion application, next to the branding logo. You can tap this icon on Avaya Vantage™ Connect to open the companion application. You can use COMPANION_APPLICATION_BRANDING_FILE to replace the default companion application icon. For provisioning, use the **SET** command in the `46xxsettings.txt` file. For example, to set the Hudini hospitality application as the companion application of Avaya Vantage™ Connect, set the parameter as the following: `SET COMPANION_APPLICATION "com.arowana.houdini_tab_portrait"` To display the icon for Avaya Connect Expansion Module next to the branding logo when the Avaya Connect Expansion Module application is installed on the same device where Avaya Vantage™ Connect is running and it is connected with Avaya Vantage™ Connect, keep the default value for COMPANION_APPLICATION.
COMPANION_APPLICATION_BRANDING_FILE	String	Null (“”)	Specifies the URL to download the companion application icon image. Avaya Vantage™ Connect displays the companion application icon next to the branding logo on the top left corner of the application. Specify the URL using the absolute path format, where the URL must start with either `http://` or `https://`. The image must be of the following settings: • Resolution: 142x56. • File format: PNG, JPG (JPEG), GIF, or BMP. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Settings menus access parameter

Parameter	Type	Default value	Description
SETTINGS_MENUS_ACCESS	Numeric	0	Specifies whether the user or only the administrator can access settings menus on Avaya Vantage™ Connect. You can assign one of the following values: • 0: Both the user and administrator can access settings menus. • 1: Only the administrator can access settings menus using the administrator password. You must use the administrator password that is set through ADMIN_PASSWORD or PROCPSWD. In an Avaya Aura® environment, if the complex password is configured in System Manager, use that password as the administrator password. If it is not available, use ADMIN_PASSWORD or PROCPSWD. In an IP Office environment, set ADMIN_PASSWORD using the `SET_ADMINPSWD=x` NUSN, where `x` is the password that is added to the autogenerated `46xxsettings.txt` file. For example: `SET_ADMINPSWD=Avaya@1234` For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.

Hot dialing parameters

Parameter	Type	Default value	Description
HOTLINE	String	Null (“”)	Specifies zero or one hotline number. When you define a phone number in this parameter, hot dialing is enabled and Avaya Vantage™ Connect automatically makes a call to the configured number when the device goes off-hook. When the parameter value is null, hot dialing remains disabled. A valid parameter value can contain up to 30 dialable characters that can include: 0 to 9, *, and #. To autodial a number with a password, you can include a comma between the phone number and the password in the parameter value. For example: `SET HOTLINE “<extension>,<password>#”` For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
HOTLINE_CALL_TYPE	Numeric	0	Specifies the outgoing hotline call type. You can assign one of the following values: • 0: Audio call. • 1: Video call. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
HOTLINE_ADMIN_MESSAGE	String	Lift handset to place a call to Hotline number	Specifies the message to be displayed on the Home screen of Avaya Vantage™ Connect when hot dialing is enabled. On K175, the message length can be a maximum of 255 characters. On K155, the maximum length is 68 characters. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Avaya Connect Expansion Module parameters

Parameter	Type	Default value	Description
BUTTON_MODULE_ENABLE	Numeric	0	Specifies whether the Expansion Module service is enabled on Avaya Vantage™ Connect. This parameter also defines whether the Avaya Vantage™ Connect user can enable or disable the Expansion Module service through the **User Settings** menu of Avaya Vantage™ Connect. An Expansion Module application can discover, pair, and connect with Avaya Vantage™ Connect only when the Expansion Module service is enabled on Avaya Vantage™ Connect. You can assign one of the following values: • 0: The Expansion Module service is disabled on Avaya Vantage™ Connect. Avaya Vantage™ Connect does not provide an option in the **User Settings** menu to enable the service. If any Expansion Module application was already paired and connected when you change the parameter value to 0, then such connection are closed and pairing information is deleted. • 1: The Expansion Module service is always enabled on Avaya Vantage™ Connect. The Avaya Vantage™ Connect user cannot disable the service through the application's **User Settings** menu. Avaya Vantage™ Connect provides additional options to enable network discovery by Expansion Module applications. • 2: By default, the Expansion Module service is disabled on Avaya Vantage™ Connect. The Avaya Vantage™ Connect user can enable or disable the service through the application's **User Settings** menu. Avaya Vantage™ Connect provides additional options to enable network discovery by Expansion Module applications. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
BUTTON_MODULE_CONNECTION_PORT	Numeric	1389	Specifies the TCP port on which Avaya Vantage™ Connect will listen to incoming TCP connections from Expansion Module applications. The range is from 0 to 65535. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Presence settings parameters

Parameter	Type	Default value	Description
ENABLE_PRESENCE	Numeric	1	Specifies whether Avaya Vantage™ Connect supports the presence service. The application supports the presence service in both Avaya Aura® and IP Office environments. You can assign one of the following values: • 0: Presence is disabled. • 1: Presence is enabled. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
DND_SAC_LINK	Numeric	0	Specifies whether to activate the Send All Call feature when the Avaya Vantage™ Connect user changes their presence status to Do Not Disturb (DND). This parameter is supported in both Avaya Aura® and IP Office environments. You can assign one of the following values: • 0: The Send All Call feature is not activated when the user changes the presence status to DND. • 1: The Send All Call feature is activated when the user changes the presence status to DND. Avaya Vantage™ Connect sends all incoming calls to the users voice mail. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
AUTO_AWAY_TIME	Numeric	10	Specifies the idle time in minutes until the presence status automatically changes to Away. The parameter value that you specify is normalized down to one of the following numbers that is the nearest: 0, 5, 10, 15, 30, 60, 90, 120. A value of 0 disables the feature. This parameter is supported only in an Avaya Aura® environment. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. • The application's **User Settings** menu.

IP Office parameters

When used as a file server, the IP Office system automatically generates the `46xxsettings.txt` file with the parameters that specify the settings of the Avaya Vantage™ device. The automatically generated `46xxsettings.txt` file includes parameter settings that are required for IP Office operation, including those that are automatically adjusted to match the configuration of the IP Office system. Avaya recommends that you do not modify the automatically generated settings file.

The automatically generated settings file does not include all the settings for Avaya Vantage™; for example, the emergency numbers. If the Lock mode is enabled, for the device user to be able to make an emergency call from a locked device, you must configure the location-specific emergency numbers in the `46xxspecials.txt` file. When enabled, you can use the `46xxspecials.txt` file for additional device settings or override selected settings in the automatically generated file. For more information about using a `46xxspecials.txt` file, see *Avaya IP Office™ Platform SIP Telephone Installation Notes*.

The following table lists a subset of IP Office core settings parameters that are supported on Avaya Vantage™.

Parameter	Type	Default value	Description
ENABLE_IPOFFICE	Numeric	0	Specifies whether the deployment environment is IP Office. The parameter takes one of the following values according to the deployment environment: • 0: Non IP Office environment. • 1: IP Office environment. For provisioning, use the **SET** command in the settings file.
ENABLE_AVAYA_ENVIRONMENT	Numeric	1	Specifies whether the device is configured for use in an Avaya or a third-party proxy environment. You can assign one of the following values: • 0: The device operates in a mode to comply with third-party SIP proxy provisioning with SIPPING-19. For IP Office and Open SIP environments, use this value. • 1: The device operates in the Avaya environment with advanced SIP telephony features and PPM.
DISCOVER_AVAYA_ENVIRONMENT	Numeric	1	Specifies whether the device should discover and verify if the SIP controller supports Advanced SIP Telephony (AST) feature set. You can assign one of the following values: • 0: The device operates in a mode where AST features are not available. For IP Office and Open SIP environments, use this value. • 1: The device determines whether the SIP controller supports AST features in the Avaya environment. If the device receives a positive response, then it synchronizes with PPM. If synchronization. If the device does not receive a response, it operates in a mode where AST features are not available.
SIMULTANEOUS_REGISTRATIONS	Numeric	3	Specifies the number of Session Manager instances with which the device can simultaneously register. The range is from 1 to 3. In an IP Office environment, the value of the parameter is set to 1.
REGISTERWAIT	Numeric	900	Specifies the number of seconds between re-registrations with the current server. Valid values are from 30 to 86400.

Table continues…

Parameter	Type	Default value	Description
IPO_CONTACTS_ENABLED	Numeric	0	Specifies whether IP Office contact management is enabled for the active Avaya™ Client SDK application on Avaya Vantage™. You can assign one of the following values: • 0: IP Office contact management is disabled for the Avaya™ Client SDK application. • 1: IP Office contact management is enabled for the Avaya™ Client SDK application. In an IP Office environment, the value of the parameter must be set to 1.
ENABLE_IPO_CALL_LOG	Numeric	0	Specifies whether the Centralized Call Logs feature is enabled or whether only local calls logs are used by the Avaya™ Client SDK application. You can assign one of the following values: • 0: The Centralized Call Logs feature is disabled for the Avaya™ Client SDK application. Only local calls logs are accessible. • 1: The Centralized Call Logs feature is enabled for the Avaya™ Client SDK application.
PSTN_VM_NUM	String	Null	Specifies the telephone number to be dialed automatically when the telephony user presses the **Messaging** button. The specified number is used to connect to the user's voice mail system. PSTN_VM_NUM is used with IP Office and third-party SIP call control environments instead of MSGNUM.
SUBSCRIBE_LIST_NON_AVAYA	String	reg, message-summary, avaya-ccs-profile	Specifies a comma-separated list of event packages to subscribe to after registration. Possible values: reg, dialog, mwi, ccs, message-summary, and avaya-ccs-profile. The values are not case sensitive. For IP Office, the recommended value is "reg, message-summary, avaya-ccs-profile". For a third-party SIP call control environment, the value can be set to "message-summary".

Upgrade-related parameters

If the upgrade policy parameters are changed, Avaya Vantage™ implements these changes after a reboot or the next polling.

Parameter	Type	Default value	Is set to default on reset	Description
UPGRADE_POLLING_PERIOD	Integer	60	Yes	Specifies the interval between two consecutive attempts of polling the upgrade files and the settings files. The polling interval is measured in minutes. Assign one of the following values: • 0: Polling is disabled. • 5 to 10080: Polling is enabled. The minimum polling interval you can define is 5 minutes. The parameter value range supported by Avaya Vantage™ is 0, 5-10080. If you define a value from 1 to 4, Avaya Vantage™ considers it as invalid and takes the default value of 60 minutes. In each polling, the upgrade files and the settings files are downloaded if modified. If any change is identified to the settings file, then the device applies the new settings. The device checks whether a newer version of the firmware is available on the file server. If a newer version is detected, then it is downloaded and installed according to the upgrade rules defined by the parameters UPGRADE_POLICY, UPGRADE_DLOAD_START, UPGRADE_DLOAD_END, UPGRADE_INSTALL_DATE_TIME, DLOAD_RND_AFTER_RESET, and DLOAD_RND. If the UPGRADE_POLICY value is 0, then UPGRADE_POLLING_PERIOD is ignored. The upgrade and settings files are downloaded only after a reboot. For upgrades to take place immediately after a polling, you must set UPGRADE_POLICY to 2. UPGRADE_POLLING_PERIOD is not affected by UPGRADE_DLOAD_START and UPGRADE_DLOAD_END parameters. Also, this parameter has no effect on any ad hoc upgrade command that is triggered by the management application or through the device UI. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
UPGRADE_POLICY	Integer	0	Yes	Specifies the upgrade policy. Assign one of the following values: • 0: Avaya Vantage™ downloads and installs the firmware files after a reboot only. The device does not automatically poll the server for upgrade and configuration files at intervals. For IP Office deployments, use this value. • 1: Avaya Vantage™ downloads and installs the firmware files according to upgrade policy rules and management application settings. Avaya Vantage™ does not perform the upgrade after a reboot. • 2: Avaya Vantage™ downloads and installs the firmware files after any reboot and according to upgrade policy rules and management application settings. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
UPGRADE_DLOAD_START	String	00	Yes	Specifies a time when Avaya Vantage™ starts trying to download new upgrade image files. The value of parameter is a string in the `[Ddd]hh` format, where: • `[Ddd]` is a day of the week. The valid values are `Sun`, `Mon`, `Tue`, `Wed`, `Thu`, `Fri`, or `Sat`. This component is optional. If the component is omitted, Avaya Vantage™performs polling every day. • `hh` is one or two numeric digits representing the hour of the day. The range is from 0 to 23. If the value of UPGRADE_DLOAD_START is equal to the value of UPGRADE_DLOAD_END, then no polling period is specified and Avaya Vantage™ can download upgrade files at any time. UPGRADE_DLOAD_START and UPGRADE_DLOAD_END are ignored if UPGRADE_POLICY is set to 0. These parameters are applicable only when UPGRADE_INSTALL_DATE_TIME is configured to a *future* date. For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.
UPGRADE_DLOAD_END	String	00	Yes	Specifies a time when Avaya Vantage™ stops trying to download new upgrade image files. Even after the specific time is up, any ongoing file downloads are taken to completion. However, new file downloads are scheduled for the next download timeframe. The value of the parameter uses the `[Ddd]hh` format, where: • `[Ddd]` is a day of the week. The valid values are `Sun`, `Mon`, `Tue`, `Wed`, `Thu`, `Fri`, or `Sat`. This component is optional. If the component is omitted, Avaya Vantage™performs polling every day. • `hh` is one or two numeric digits representing a hour of the day. The range is from 0 to 23. For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
UPGRADE_INSTALL_DATE_TIME	String	1970-01-01T00:00	Yes	Specifies the date and time when Avaya Vantage™ starts to install the downloaded upgrade files. The value of the parameter uses the `YYYY-MM-DDThh:mm` format, where: • `YYYY` is four numeric digits representing the year • `MM` is two numeric digits representing the month. • `dd` is two numeric digits representing the day of the month. • `T` is the time separator. • `hh` is two numeric digits representing a hour of the day. The range is from 0 to 23. • `mm` is two numeric digits representing minutes of the hour. The range is from 0 to 59. If the default value is used or the value is set to a past date and UPGRADE_POLICY is set to 2, Avaya Vantage™ installs upgrade files immediately after downloading irrespective of other parameter definitions. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
DLOAD_RND_AFTER_RESET	Integer	0	Yes	Specifies the maximum length of the interval Avaya Vantage™ waits after reboot before attempting to download the upgrade files. The interval is measured in seconds. Assign one of the following values: • 0: The interval is not specified. Avaya Vantage™ starts the download immediately after reboot. • 1 – 32767: After reboot, Avaya Vantage™ delays the download. The exact delay interval is determined as a random number in a range between 0 and the DLOAD_RND_AFTER_RESET value. Avaya recommends that you configure randomized download time in an environment where multiple devices access the file server at the same time. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
DLOAD_RND	Integer	3600	Yes	Specifies the maximum length of an interval between two consecutive attempts of background downloading. The interval is measured in seconds. Assign one of the following values: • 0: The interval is not specified. Avaya Vantage™ performs background download attempts without delay. • 1 – 32767: Avaya Vantage™ inserts a delay between two background download attempts. The exact delay interval is determined as a random number in a range between 0 and the DLOAD_RND value. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ENABLE_CORDLESS_HANDSET_UPDATE	Integer	0		Specifies whether the wireless handset upgrade is enabled. Assign one of the following values: • 0: To disable the wireless handset upgrade. • 1: To enable the wireless handset upgrade. Avaya Vantage™ applies the update automatically whenever an update is available on the file server. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Protocol-specific parameters

Captive portal

Parameter	Type	Default value	Is set to default on reset	Description
CAPTIVE_PORTAL_SERVER	String	connectivitycheck.gstatic.com	Yes	Specifies the URL of the captive portal server for HTTP authentication to use the Internet. Use the `[http://]hostname[:port][/path]` format, where: • `hostname` is either an IP address in the dotted decimal format or a domain name. • `port` is an optional port number. • `path` is an optional path to the server. If you want to disable the detection mechanism, use the null string as the parameter value. For provisioning, use: • DHCP option 242. • The **SET** command in the `46xxsettings.txt` file.

TLS

Parameter	Type	Default value	Is set to default on reset	Description
TLSSRVRID	Integer	1	Yes	Specifies whether the TLS server identification is required. Assign one of the following values: • 0: Certificate validation is not required. TLS connection is established in all cases. • 1: Certificate match required. TLS connection is established only if the server identity matches the servers certificate. For provisioning, use: • DHCP option 43. • The **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
TLS_VERSION	Numeric	1	Yes	Specifies which TLS versions are supported with all TLS connections used by Android and Avaya applications. Assign one of the following values: • 0: TLS versions 1.0 and 1.2 are supported. • 1: TLS version 1.2 only is permitted. From Release 2.2.0.3 onwards, the default value of TLS_VERSION is 1. Before upgrading to Release 2.2.0.3, ensure that all services that connect with Avaya Vantage™ using TLS support TLS 1.2. If any services do not support TLS 1.2, upgrade them to support TLS 1.2. Otherwise, you can change the value of TLS_VERSION to 0. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

LLDP

Parameter	Type	Default value	Is set to default on reset	Description
LLDP_ENABLED	Integer	1	Yes	Specifies whether LLDP is enabled. Assign one of the following values: • 0: Disabled. • 1: Enabled. • 2: Enabled. Avaya Vantage™ starts to transmit LLDP frames only after receiving of an LLDP frame. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Security parameters

Certificate configuration parameters

The following parameters are for managing download and usage of trusted and general certificates on Avaya Vantage™.

Parameter	Type	Default value	Is set to default on reset	Description
TRUSTCERTS	String	null string	Yes	Specifies file names of trusted certificates to be used for authentication. The parameter supports both root and intermediate certificates. Avaya Vantage™ supports certificates both in the PEM and DER file formats. If you are providing several file names, use commas to separate them. You can upload up to 100 trusted certificates on Avaya Vantage™. The maximum length of the parameter value is 1024 characters for firmware release 2.1 or earlier. For firmware release 2.2 and later, the length of the parameter value can be up to 4000 characters. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. Example: `SET TRUSTCERTS SMGRCA.cer,Entrust.cer,Digicert.cer` If you configure TRUSTCERTS in the `46xxsettings.txt` file and provide relative file paths in the value, Avaya Vantage™ downloads the certificate files from the HTTP or HTTPS file server defined in FILE_SERVER_URL, HTTPSRVR, or TLSSRVR. If you define TRUSTCERTS in Avaya Aura® Device Services, you must provide absolute URLs to the certificate files. TRUSTCERTS configuration using Avaya Aura® Device Services gets a higher precedence than `46xxsettings.txt`. When using Avaya Aura® Device Services, you must ensure that the TRUSTCERTS parameter value defined in the `46xxsettings.txt` file has the same set of certificates as the value defined in Avaya Aura® Device Services. However, the syntax does not need to be the same. The certificate file paths or the order of the certificates in the list need not be the same in the parameter value in the `46xxsettings.txt` file and Avaya Aura® Device

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
				Services. Also, you must include the root CA of the Avaya Aura® Device Services server identity certificate in the TRUSTCERTS parameter value.
MYCERTURL	String	null string	Yes	Specifies the URL for the Simple Certificate Enrollment Protocol (SCEP) server. Avaya Vantage™ attempts to contact the server if the parameter value is not the default. A valid URL must start with `http://`. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
MYCERTCN	String	$SERIALNO	Yes	Specifies the Common Name (CN) for SUBJECT in a SCEP certificate request. If the parameter value contains the `$SERIALNO` string, Avaya Vantage™ replaces this string with the device serial number. If the parameter value contains the `$MACADDR` string, Avaya Vantage™ replaces that string with the device MAC address. **Note:** The parameter value must not contain the `*` symbol. If the parameter value contains this symbol, Avaya Vantage™ considers the value to be invalid. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
MYCERTDN	String	Null	Yes	Specifies the common part of SUBJECT in a SCEP certificate request. This value defines the part of SUBJECT that is common for requests from different devices, such as Organizational Unit, Organization, Location, State, and Country. The parameter value must start with the slash (`/`) symbol. **Note:** Do no use the asterisk (`*`) symbol. If the value contains this symbol, Avaya Vantage™ considers the value to be invalid. For example: `/C=US/ST=CA/L=MILPITAS/O=Avaya`

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
				For provisioning, use the **SET** command in the `46xxsettings.txt` file.
MYCERTKEYLEN	Integer	2048	Yes	Specifies the RSA private key length in bits. The private key is used on the device for certificate enrollment. Avaya Vantage™ only supports keys with a length of 2048 bits. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
MYCERTCAID	String	CAIdentifier	Yes	Specifies the Certificate Authority Identifier (CAI). Certificate Authority servers might require a specific CAI string in order to accept GetCA requests. If Avaya Vantage™ works with such a Certificate Authority, the CA identifier string must be set through this parameter. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
SCEPPASSWORD	String	$SERIALNO	Yes	Specifies a password to use with SCEP. The non-null value of SCEPPASSWORD is included in a challengePassword attribute in SCEP certificate signing requests. If the value contains $SERIALNO, $SERIALNO is replaced with the value of SERIALNO. If the value contains $MACADDR, $MACADDR is replaced with the value of MACADDR without the colon separators. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** menu on the device.
MYCERTREPLACE	Numeric	90	Yes	Specifies the period of the certificate's validity interval. This period is specified as a percentage. Avaya Vantage™ uses this percentage to calculate the date of the certificate replacement before its expiration. When the configured period is over, Avaya Vantage™ tries to download the newest version of the certificate from the SCEP server. The range is from 1 to 99. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
ENABLE_PUBLIC_CA_CERTS	Numeric	0	Yes	Specifies whether embedded Android trusted certificates are used by application services, such as Avaya Aura® Device Services, PPM, 802.1x EAP-TLS, SCEP, and file downloads using HTTPS. You can assign one of the following values: • 0: The services do not use embedded Android trusted certificates. • 1: The services use embedded Android trusted certificates. In the following cases, this parameter is enforced to 1 even if it was configured as 0: • When Avaya Vantage™ is installed in a Device Enrollment Services environment. • When Avaya Vantage™ obtains the provisioning server address from a redirect from Device Enrollment Services. • When Device Enrollment Services was used before and no private CA is retrieved from Device Enrollment Services. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
CA_CERT_BLACKLIST	String	Null	Yes	Specifies a list of comma-separated SHA-1 signatures of Android embedded trusted certificates, which must be blocked. Use this parameter to disable specific trusted certificates due to certificate revocation or if you do not trust the certificate. Only add certificates that are not already disabled in Android. You can find the list of these certificates in the `/data/misc/keychain/pubkey_blacklist.txt` file. This parameter can contain up to 1024 characters. For provisioning, use the **SET** command in the `46xxsettings.txt` file. For example: `SET CA_CERT_BLACKLIST 410f36363258f30b347d12ce4863e433437806a8,c4f9663716cd5e71d6950b5f33ce041c95b435d1`

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
PKCS12URL	String	Null	Yes	Specifies the URL to be used to download a PKCS #12 file. This file contains an identity certificate and its private key. The parameter value can contain up to 255 ASCII characters. The address can contain the following options: • $SERIALNO: This options is replaced with the Avaya Vantage™ serial number • MACADDR: This option is replaced with the Avaya Vantage™ MAC address without colons For example: An Avaya Vantage™device has the 00-24-D7-E4-2E-98 MAC address. The URL of the PKCS file is specified as `http://<path_to_the_file>/pkc12file_$MACADDR.cer`. In this case, the PKCS file for the device must have the `pkc12file_0024D7E42E98` name. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
PKCS12PASSWORD	String	Null	Yes	Specifies a PKCS #12 file password. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** menu on the device.
PKCS12_PASSWD_RETRY	String	3	Yes	Specifies the number of failed attempts to enter the password for the PKCS#12 file. If the user fails to enter the correct password, Avaya Vantage™ will not install the PKCS#12 file. The range is from 0 to 100, where 0 means that the user cannot retry to enter the password. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
ID_CERT_APPLICATION_LIST	String	all	Yes	Specifies which applications can access the identity certificate stored on Avaya Vantage™. Assign one of the following values: • all: All applications can access certificates. • Null string: No application can access certificates. The exception is an active phone application

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
				defined in ACTIVE_CSDK_BASED_PHONE_APP. • A list of comma-separated application package names: Only the specified applications can access certificates. For example: `SET ID_CERT_APPLICATION_LIST flare.avaya.com,vantage.basic.avaya.com` For provisioning, use the **SET** command in the `46xxsettings.txt` file.
DELETE_MY_CERT	String	0	Yes	Specifies whether Avaya Vantage™ should delete the installed identity certificate. Assign one of the following values: • 0: The installed identity certificate remains on the system. • 1: The installed identity certificate will be deleted from the system. For provisioning, use: • DHCP option 242. • The **SET** command in the `46xxsettings.txt` file.
CERT_WARNING_DAYS	Numeric	60	Yes	Specifies the number of days before the certificate expiry date when Avaya Vantage™ starts to display certificate expiration warning messages. Avaya Vantage™ displays the warning message every seven days. This parameter relates to trusted certificates, OSCP certificates, EASG certificates, and the identity certificate. The range is from 0 to 99. If the value set to 0, Avaya Vantage™ does not display certificate expiration warning messages. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
EASG_SITE_CERTS	String	null string	Yes	Specifies EASG site certificate file names. These certificates are used by technicians when they do not have access to the Avaya network to generate EASG responses for SSH login. The value of the parameter is a list of file names separated by commas without any spaces between

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
				entries. The value can contain up to 255 ASCII characters. To delete the EASG trusted certificate from the device, remove the corresponding file name from EASG_SITE_CERTS. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
EASG_SITE_AUTH_FACTOR	String	null string	Yes	Specifies the EASG site authentication factor code associated with the EASG site certificate. The value of the parameter can contain from 10 to 20 alphanumeric characters. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

SELinux settings

Parameter	Type	Default value	Is set to default on reset	Description
SELINUX_MODE	Numeric	1	N/A	Specifies the SELinux mode. • 0: Sets the permissive mode. • 1: Sets the enforcing mode. Setting the SELinux mode triggers a device reset. End users get the option to restart the device immediately or later. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

FIPS mode parameter

Parameter	Type	Default value	Description
FIPS_ENABLED	Numeric	0	Specifies whether only FIPS-approved cryptography algorithms are supported on Avaya Vantage™. • 0: Disables FIPS mode. No restriction on using non FIPS-approved cryptography algorithms by services. • 1: Enables FIPS mode. Services can use only FIPS-approved cryptography algorithms. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

General account IDs & passwords

Parameter	Type	Default value	Is set to default on reset	Description
SIPUSERNAME	String	Null	Yes	Specifies the user's account to register on a SIP server. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. For provisioning, use: • Enter the user account name on the Login screen. • Use the **SET** command in the settings file from Avaya Aura® Device Services. The `46xxsettings.txt` file from the HTTP or HTTPS server is not supported.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
SIPPASSWORD	String	Null	Yes	Specifies the user's password used to register on a SIP server. The parameter value can contain up to 255 alphanumerical characters. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. For provisioning: • Enter the user account name on the Login screen. • Use the **SET** command in the settings file from Avaya Aura® Device Services. The `46xxsettings.txt` file from the HTTP or HTTPS server is *not* supported.
SIPHA1	String	Null	Yes	Specifies the HA1 hash value of the user's password used to register on a SIP server. HA1 is calculated as MD5 (username:domain:password). The parameter value can contain up to 255 alphanumerical characters. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. This parameter is only configurable from Avaya Aura® Device Services. The `46xxsettings.txt` file from the HTTP or HTTPS server is *not* supported.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
PROCPSWD	Numeric	27238	Yes	Specifies the password required to access administrator menu options in the **Settings** menu on Avaya Vantage™. The parameter value can contain 4 to 7 numeric characters. If both PROCPSWD and ADMIN_PASSWORD have default values, you cannot access administrator options in the **Settings** menu. In an Avaya Aura® environment, if the complex password is configured in System Manager for the specific device location, Avaya Vantage™ uses the complex password as the administrator password and ignores ADMIN_PASSWORD and PROCPSWD. If it is not available, Avaya Vantage™ uses ADMIN_PASSWORD. Otherwise, it uses PROCPSWD. For provisioning, use: • A `name=value` pair in a DHCPACK message. • The **`SET`** command in the `46xxsettings.txt` file. • The value stored on the PPM server.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
ADMIN_PASSWORD	String	Null	Yes	Specifies a complex password required to access administrator menu options in the **Settings** menu on Avaya Vantage™. A valid value can contain 6 to 31 alphanumeric characters including upper and lower case letters, numbers, and special characters. Do not use the double quotation mark as a special character in the value. • In an Avaya Aura® environment, if the complex password is configured in System Manager for the specific device location, Avaya Vantage™ uses the complex password as the administrator password and ignores ADMIN_PASSWORD and PROCPSWD. If it is not available, Avaya Vantage™ uses ADMIN_PASSWORD. Otherwise, it uses PROCPSWD. • If ADMIN_PASSWORD is configured, Avaya Vantage™ ignores PROCPSWD. • If ADMIN_PASSWORD has the default value, Avaya Vantage™ uses PROCPSWD to provide access to administrator options in the **Settings** menu. If both ADMIN_PASSWORD and PROCPSWD have default values, you cannot access administrator menu options in the **Settings** menu. For provisioning, use the **`SET`** command in the `46xxsettings.txt` file. In an IP Office environment, set ADMIN_PASSWORD using the `SET_ADMINPSWD=x` NUSN, where `x` is the password that is added to the autogenerated `46xxsettings.txt` file. For example: `SET_ADMINPSWD=Avaya@1234`

Login screen specific parameters

Parameter	Type	Default value	Description
SHOW_LAST_EXTENSION	Numeric	0	Specifies whether to present the SIP extension or unified login user name on the Login screen after you log out or tap **Cancel** during a login operation. • 0: The SIP extension or unified login user name is not displayed on the Login screen. • 1: The SIP extension or unified login user name is displayed on the Login screen. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
PRESERVE_LOGIN_PASSWORD	Numeric	0	Specifies whether to preserve the SIP or unified login password on the Login screen after you tap **Cancel** during a login operation. • 0: The password is not preserved on the Login screen. • 1: The password is preserved on the Login screen. The password is always masked. This parameter is only applicable if you set SHOW_LAST_EXTENSION as 1. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Device lock and idle time parameters

Parameter	Type	Default value	Description
ENABLE_PHONE_LOCK	Numeric	0	Specifies whether the Lock screen is enabled on the device. • 0: The Lock screen is disabled. • 1: The Lock screen is enabled. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** menu on the device.
PHONE_LOCK_IDLE TIME	Numeric	60	Specifies the maximum interval of idle time in minutes after which Avaya Vantage™ is locked automatically. The range is from 1 to 10080. Avaya Vantage™ ignores this parameter if ENABLE_PHONE_LOCK is 0. The user can choose a smaller idle time than this parameter value in the **Settings** > **Security & location** > **Automatically lock** menu. Avaya Vantage™ uses this parameter value to determine the number of options it shows to the user in the **Settings** > **Security & location** > **Automatically lock** and **Settings** > **Display** > **Sleep** menus. By default, the **Automatically lock** and **Sleep** fields have the following options: 1, 2, 5, 10, 30 minutes, 1 hour, 2 hours, 5 hours, 10 hours, 1 day, 2 days, and 1 week. The minimum value is 1 minute. The maximum value is the minimum value between the PHONE_LOCK_IDLETIME value and the value specified by the Exchange policy. For example, if the PHONE_LOCK_IDLETIME value is 145 and the value specified by the Exchange policy is 123 minutes, then the **Automatically lock** field provides options from 1 minute to 2 hours inclusively. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Description
PHONE_LOCK_PASSWORD_FAILED_ATTEMPTS	Numeric	8	Specifies the number of failed login attempts before Avaya Vantage™ becomes locked. The range is from 8 to 20. If the parameter set to 0, then the number of failed attempts is unlimited. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. For provisioning, use the **`SET`** command in the `46xxsettings.txt` file.
LOCK_SCREEN_LOCK_AFTER_TIMEOUT	Numeric	5	Specifies the Lock screen inactivity timeout in minutes. The range is from 1 to 10080. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. For provisioning, use the **Settings** menu on the device.
ALLOW_LOGOUT_WHEN_LOCKED	Numeric	1	Specifies whether users can log out from the Lock screen. Assign one of the following values: • 0: A user cannot perform logout when the device is locked. • 1: A user can perform logout from the Lock screen. • 2: When device is locked, an administrator can perform logout through the **Settings** menu only. In addition, the logout option is available only for administrator when the device is unlocked and logged in. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. For provisioning, use: • The **`SET`** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

Parameters to lock and obscure Settings menu options

Parameter	Type	Default value	Description
LOCKED_PREFERENCES	String	Null	Specifies the list of parameters to be locked from user modification in the device **Settings** menu. The user can only view the values of these parameters but cannot modify them. The value of the LOCKED_PREFERENCES parameter is a list of parameter names. Separate the names in the list using commas without any space after each comma. The following is the list of parameters that you can specify in the list: • DHCP_SSON: The site-specific option number for DHCP. • FILE_SERVER_URL: The file server address for downloading firmware and configuration files. • GROUP: The identifier for a set of configuration parameters in the `46xxsettings.txt` file that are specific to the user group. • DNSSRVR: IP addresses of DNS servers. • DOMAIN: The DNS server domain name. • SIPDOMAIN: The SIP domain name used for SIP registration. • SIP_CONTROLLER_LIST: Addresses of SIP proxy or registrar servers. • IPADD: IP address, netmask, and router information of the Avaya Vantage™ device. • L2Q and L2QVLAN: VLAN information. • SNTPSRVR: Addresses of SNTP servers. The LOCKED_PREFERENCES parameter does not affect your access to the **Settings** menu options if you are the administrator. For provisioning, use: • The **`SET`** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

Table continues…

Parameter	Type	Default value	Description
OBSCURE_PREFERENCES	String	Null	Specifies the list of parameters to be hidden from users in the device **Settings** menu. The value of the OBSCURE_PREFERENCES parameter is a list of parameter names. Separate the names in the list using commas without any space after each comma. The following is the list of parameters that you can specify in the list: • DHCP_SSON: The site-specific option number for DHCP. • FILE_SERVER_URL: The file server address for downloading firmware and configuration files. • GROUP: The identifier for a set of configuration parameters in the `46xxsettings.txt` file that are specific to the user group. • DNSSRVR: IP addresses of DNS servers. • DOMAIN: The DNS server domain name. • SIPDOMAIN: The SIP domain name used for SIP registration. • SIP_CONTROLLER_LIST: Addresses of SIP proxy or registrar servers. • IPADD: IP address, netmask, and router information of the Avaya Vantage™ device. • L2Q and L2QVLAN: VLAN information. • SNTPSRVR: Addresses of SNTP servers. The OBSCURE_PREFERENCES parameter does not affect your access to the **Settings** menu options if you are the administrator. For provisioning, use: • The **`SET`** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

Important:

In an environment with Avaya Aura® Device Services, if the global **Lock settings** and **Obscure locked settings** options in Avaya Aura® Device Services are in the enabled state, Avaya Vantage™ ignores the preferences defined in the LOCKED_PREFERENCES and OBSCURE_PREFERENCES settings. For the LOCKED_PREFERENCES and OBSCURE_PREFERENCES settings to take effect, you must disable the global settings in Avaya Aura® Device Services.

Emergency call settings

The following table describes which parameters to configure for location-specific emergency numbers.

Parameter	Type	Default value	Is set to default on reset	Description
PHNEMERGNUM	String	Null string	Yes	Specifies the emergency number with the highest priority. Avaya Vantage™ dials this number when a user taps **Auto - dial** for an emergency call. The parameter value can contain up to 30 characters. You can use `0-9`, `*`, and `#` characters. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. With IP Office, set this parameter in the `46xxspecials.txt` file. In an Avaya Aura® deployment, configure emergency numbers in the PPM server. Do not use this parameter.
PHNMOREEMERGNUMS	String list	Null string	Yes	Specifies an additional list of emergency numbers. The value of the parameter is a list of emergency numbers separated by commas without any spaces between entries. The parameter value can contain up to 100 numbers. Each number can contain up to 30 characters. You can use `0-9`, `*`, and `#` characters. This parameter is *not* supported in the non Avaya™ Client SDK application based mode. With IP Office, set this parameter in the `46xxspecials.txt` file. In an Avaya Aura® deployment, configure emergency numbers in the PPM server. Do not use this parameter.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
ENABLE_PUBLISH_MAC_ADDRESS	Numeric	0		Specifies whether to publish the MAC address of the Avaya Vantage™ device in all SIP signaling and PPM messages. PPM is supported in the Avaya Aura® environment only. You can assign one of the following values: • 0: SIP signaling and PPM messages do not include the MAC address of the device. • 1: SIP signaling and PPM messages include the MAC address of the device. Depending on the active network interface, the Ethernet or Wi-Fi MAC address is published in the SIP REGISTER messages. When you enable this option, a third-party location service can use the device's MAC address to determine and report the location of the device for emergency calls. For correct reporting of the Ethernet MAC address of the device in System Manager, you must set ENABLE_PUBLISH_MAC_ADDRESS to 1. With Avaya Aura®, use one of the following provisioning options: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. With IP Office, set this parameter in the `46xxspecials.txt` file.

Logging and debugging parameters

Event log settings

Parameter	Type	Default value	Is set to default on reset	Description
LOGSRVR	String	Null	Yes	Specifies an address of a server where syslog messages are stored. For Avaya Vantage™, you can define the IP address of the syslog server in the dotted decimal or DNS format. The parameter value can have up to 255 characters. For provisioning, use: • DHCP option 7 in a DHCPACK message. • The **Settings** menu on the device.
SYSLOG_ENABLED	Integer	0	Yes	Specifies whether Avaya Vantage™ generates syslog messages. Assign one of the following values: • 0: Syslog messages are disabled. • 1: Syslog messages are enabled. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** menu on the device.
SYSLOG_LEVEL	Integer	3	Yes	Specifies the severity level of syslog messages. Avaya Vantage™ sends a syslog message if a severity level of an event is equal or less than the value specified in this parameter. Assign one of the following values: • 3: Error • 4: Warning • 5: Notice • 6: Informational • 7: Debug For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** menu on the device.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
LOCAL_LOGS_ENABLED	Integer	1	Yes	Specifies whether Avaya Vantage™ stores log messages. Assign one of the following values: • 0: Local log storage is disabled. • 1: Local log is storage is enabled. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** menu on the device.
LOCAL_LOG_LEVEL	Integer	4	Yes	Specifies the severity level for local log messages. Avaya Vantage™ stores a log message if a severity level of an event is equal or less than the value specified in this parameter. Assign one of the following values: • 3: Error • 4: Warning • 5: Notice • 6: Informational • 7: Debug For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** menu on the device.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
LOG_CATEGORY	String	ALL	Yes	Specifies a list of logging categories. The parameter value is a list of comma-separated keywords representing logging categories. Logging implementation blocks all traces at the Warning or lower severity levels unless the category corresponding to a given trace is enabled. The device filters all ANDROID and KERNEL syslog or log categories in the following cases: • You do not configure this parameter for these categories. • The parameter value is not set to ALL. If the log level is set to Warning or a lower level, this parameter enables low-level traces from adaptors or managers. This parameter applies to both syslog and local logging mechanisms. The supported categories are: ALL, ANDROID, 8021X, ADAPMGR, CERTMGMT, CONFIG, CONFIG_MULTI, CORE, DATETIME, DAVDATA, DEVICE, DHCP, EEPROMDATA, ENCRYPT, EXTAPP, FAILOVER, FAVORITE, HISTORY, HTTP, KERNEL, LLDP, LOCALDATA, MSGMGR, MSG_ROUTING, NETADAP, NETMGR, ONEXPAUCDATA, PERSLABELS, PLATFORM_COMP, PPMDATA, PPMMESSAGE, POWER, QOS, SCRIPT, SCRIPTDATA, SECURITY, SSHDADAP, THREADWDOG, UI, UPGRADE, VMM, and WEB. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** menu on the device.

For additional event log parameters that are supported by the CSDK-based applications, see Avaya Client SDK application parameters on page 246.

Debug report settings

Parameter	Type	Default value	Is set to default on reset	Description
BRURI	String	Null		Specifies the URI of the HTTP server where the debug and audio debug reports can be saved. You can specify the server URL in the following format: `http://[username:password]hostname[:port][/path]` • `username:password` are optional HTTP server authentication credentials. • `hostname` is either an IP address in the dotted decimal format or an FQDN. • `port` is an optional port number. • `path` is an optional path to the directory where the reports are to be stored on the server. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.
DEBUG_REPORT_PASSWORD	String	Null		Specifies the encryption password for debug and audio debug reports that you can generate on Avaya Vantage™. When defined, the debug report and audio report encryption password is populated automatically. The device user cannot change this password when generating a debug report. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. For security reasons, Avaya recommends that you configure this parameter in the `46xxsettings.txt` file only when the configuration file is downloaded from the HTTP or HTTPS file server or redirected through Device Enrollment Services and there is mutual certificate authentication.

Audio debug recording settings

Parameter	Type	Default value	Is set to default on reset	Description
ENABLE_RECORDING	Integer	0	Yes	On Avaya Vantage™, this parameter controls whether audio recording is enabled as part of the audio report. Assign one of the following values: • 0: Audio debug recording is disabled. • 1: Audio debug recording is enabled. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

SSH settings

Note:

The SSH server settings on the endpoints are used by Avaya Services for debugging purposes only.

Parameter	Type	Default value	Is set to default on reset	Description
SSH_ALLOWED	Integer	0	Yes	Specifies whether the Secure Shell (SSH) is enabled. Assign one of the following values: • 0: Disabled. • 1: Enabled, with challenge and response authentication. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** menu on the device.
SSH_BANNER_FILE	String	Null	Yes	Specifies a file name or URL of a file containing a warning message. This message is displayed on a SSH client before authentication. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
SSH_IDLE_TIMEOUT	Integer	10	Yes	Specifies the number of minutes of inactivity after which an SSH connection is terminated. The range is from 0 to 32767. Assign one of the following values: • 0: No timeout. • 1 –32767: Number of minutes of inactivity after which SSH is disabled. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
SSH_ROOT_ALLOWED	Numeric	0	Yes	Specifies whether sroot access is allowed. Assign one of the following values: • 0: sroot access is disabled. • 1: sroot access is enabled. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The **Settings** menu on the device.

ADB settings

Parameter	Type	Default value	Is set to default on reset	Description
ADBSTAT	Numeric	1	Yes	Specifies whether Android Debug Bridge (ADB) is enabled for application development purpose on Avaya Vantage™. • 0: ADB is disabled and the option to enable ADB from the **Settings** menu of the device is disabled. • 1: ADB is disabled, but you can enable it from the **Settings** > **Developer options** > **Debugging** menu. Since ADB is a non-secure protocol, Avaya recommends that you enable ADB for Android application development only. Otherwise, set ADBSTAT to 0. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

SLA Mon™ agent settings

The following table provides the details of the parameters that you can set to enable SLA Mon™ agent and define how the SLA Mon™ features will work on the device.

Parameter	Type	Default value	Is set to default on reset	Description
SLMSTAT	Numeric	0	Yes	Specifies whether the SLA Mon™ agent is enabled on Avaya Vantage™. When you enable the agent, the SLA Mon™ server can discover the agent and use the agent in network monitoring and endpoint diagnostics. You can assign one of the following values: • 0: The SLA Mon™ agent is disabled. • 1: The SLA Mon™ agent is enabled. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
SLMSRVR	String	Null	Yes	Specifies the IP address of the SLA Mon™ server from which discovery messages shall be received for agent registration. If you enable the SLA Mon™ agent, the SLMSRVR value is mandatory. The IP address must be in the dotted decimal format, optionally followed by a colon and an integer port number from 0 to 65535. For provisioning, use the **SET** command in the `46xxsettings.txt` file.
SLMPORT	Numeric	50011	Yes	Specifies the port that is used to receive discovery and test request packets from an SLA Mon™ server. Valid values are from 0 to 65535. For provisioning, use the **SET** command in the `46xxsettings.txt` file. **Note:** If you change the default port in the settings file, you must also change the port number on the SLA Mon™ server in the `/opt/avaya/slamon/bundleconf/agentcom-slamon.conf` file.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
SLMCAP	Numeric	0	Yes	Specifies whether the SLA Mon™ agent supports packet capture. You can assign one of the following values: • 0: The packet capture feature is disabled. • 1: The packet capture feature is enabled but without payloads. • 2: The packet capture feature is enabled with RTP headers and payloads. For provisioning, use the **SET** command in the `46xxsettings.txt` file.

Additionally, you must also download the SLA Mon™ server identity root CA certificate to the device through the TRUSTCERTS parameter for server authentication. You can use a certificate issued by a Certificate Authority (CA) or an in-house CA, or use a self-signed certificate. For more information, see *Administering Avaya Diagnostic Server SLA Mon™* on the Avaya Support website.

USB parameters

Parameter	Type	Default value	Is set to default on reset	Description
ENABLE_USB_GENERAL_PURPOSE	Numeric	1	Yes	Specifies whether the USB general purpose port is enabled on the device. Assign one of the following values: • 0: To disable the USB port. You can use the USB port in the boot recovery mode. • 1: To enable the USB port. • 2: To disable the USB port both on the Android operating system and in the boot recovery mode. Avaya Vantage™ supports the value 2 as of Release 2.2.0.1. For provisioning, use the **SET** command in the `46xxsettings.txt` file. In Avaya Aura®, PPM does not back up or restore the parameter.

LDAP directory service settings

To enable or disable LDAP directory search on Avaya Vantage™ and to connect Avaya Vantage™ to the directory server, you must define the following parameters:

Parameter	Type	Default value	Is set to default on reset	Description
DIRENABLED_PLATFORM	Numeric	0	Yes	Specifies whether the LDAP directory search feature is enabled on Avaya Vantage™. You can assign one of the following values: • 0: LDAP directory search is disabled. • 1: LDAP directory search is enabled. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.
DIRUSERNAME	String	“”	Yes	Specifies the LDAP or LDAPS client authentication user name. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. Do not configure the LDAP client user name in the `46xxsettings.txt` file if you are not using the HTTPS protocol and no HTTP authentication or mutual certificate based authentication exists for the file server access. In an Avaya Aura® environment, you can use Avaya Aura® Device Services to configure this parameter securely.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
DIRPASSWORD	String	“”	Yes	Specifies the LDAP or LDAPS client authentication password. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. Do not configure the LDAP client password in the `46xxsettings.txt` file if you are not using the HTTPS protocol and no HTTP authentication or mutual certificate based authentication exists for the file server access. In an Avaya Aura® environment, you can use Avaya Aura® Device Services to configure this parameter securely.
DIRSRVR	String	Null	Yes	Specifies the IP address or fully qualified domain name (FQDN) of the LDAP directory server. Valid values are zero or more addresses separated by commas without intervening spaces. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.
DIRSRVRPRT	Numeric	636	Yes	Specifies the port number for the LDAP directory server. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
DIRTOPDN	String	Null	Yes	Specifies the LDAP search base. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. Example: **SET** `DIRTOPDN "dc=global,dc=avaya,dc=com"`
DIRSECURE	Boolean	1	Yes	Specifies whether to use TLS or TCP for LDAP. You can assign one of the following values: • 0: Use TCP. • 1: Use TLS. When you set to use TLS for LDAP, Avaya Vantage™ supports secure LDAP, that is, LDAPS. LDAPS supports both client and server authentication. For server authentication, you must add the trusted certificate to an HTTP or HTTPS server and include certificate in the TRUSTCERTS parameter value. Client authentication is based on the Avaya Vantage™ identity certificates installed using SCEP or PKCS12. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.
DIRSTARTTLS	Numeric	0	Yes	Specifies whether to use LDAPS over TLS or LDAP Start TLS (RFC 4513). You can assign one of the following values: • 0: LDAPS over TLS. • 1: LDAP Start TLS. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

Table continues…

Parameter	Type	Default value	Is set to default on reset	Description
DIRREFERRALS	Numeric	1	Yes	Specifies whether Avaya Vantage™ supports LDAP referrals. You can assign one of the following values: • 0: LDAP referrals are disabled. • 1: LDAP referrals are enabled. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

Accessibility settings

Parameter	Type	Default value	Description
ENABLE_TALKBACK	Integer	0	Specifies whether Android TalkBack is enabled on Avaya Vantage™. You can assign one of the following values: • 0: TalkBack is disabled. • 1: TalkBack is enabled. For provisioning, use: • The **SET** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services. • The **Settings** > **Accessibility** > **TalkBack** menu on the device.

Online help URL setting

Parameter	Type	Default value	Description
ONLINE_HELP_URL	String	Null string	Specifies the URL from where Avaya Vantage™ presents the device online help when a user selects **Help** in the device **Settings** menu. The value must be an absolute URL. In an Avaya Aura® deployment, the URL can also be an IPv6 address. Encapsulate the IPv6 address in brackets. For example: http://[2001:db8:85a3::8a2e]/help/ When the parameter value is null, then Avaya Vantage™ opens the Avaya Documentation Portal. Alternatively, you can download the Avaya Vantage™ device online help from the Avaya Support site and extract it to your file server. Then you can set this parameter to point Avaya Vantage™ to the local file server URL instead of the Avaya Documentation Portal. This configuration is useful if there is no internet connectivity or connection to the public network is restricted. For provisioning, use: • The **`SET`** command in the `46xxsettings.txt` file. • The settings file received from Avaya Aura® Device Services.

Appendix B: Parameter configuration examples in the settings file

Parameter configuration example for Avaya Aura® with SIP credentials

The following is a configuration example of mandatory parameters in the `46xxsettings.txt` file when the deployment environment is Avaya Aura® with SIP credentials:

```
SET TIMEZONE "America/New_York"
SET SNTPSRVR "149.12.34.567"
SET ACTIVE_CSDK_BASED_PHONE_APP "com.avaya.android.vantage.basic"
SET TRUSTCERTS "prod-sip-ca.crt"
SET SIP_CONTROLLER_LIST "135.12.345.670:5061;transport=tls"
SET SIPDOMAIN "avaya.com"
SET TLSSRVRID 0
SET USER_AUTH_FILE_SERVER_URL ""
```

The double quotes (“”) are optional for the above configuration parameter examples. However, to include spaces in a parameter value, you must enclose the value using double quotes (“”)

Some considerations while configuring parameters:

- When you are using SIP credentials, USER_AUTH_FILE_SERVER_URL must remain with the default value, which is null (“”).
- You must configure SNTPSRVR if the default Avaya and NIST SNTP servers are not accessible from the customer network. Specifying an SNTPSRVR value that is reachable from your network is essential for SIP registration and initial device setup when you start up Avaya Vantage™.
- You must set TLSSRVRID to 0 if:
  - Avaya default SIP Root CA certificates are used.
  - The identity certificate of Avaya Vantage™ services does not include Subject Alternative name with the FQDN or IP address of the services.
  - The SIP controller identity certificate does not include the correct SIP domain in Subject Alternative Name.
  - The identity certificate does not include a common name for other services.

Parameter configuration example for Avaya Aura® with user enterprise credentials

The following is a configuration example of mandatory parameters in the `46xxsettings.txt` file when the deployment environment is Avaya Aura® with user enterprise credentials:

```
SET TIMEZONE "America/New_York"
SET SNTPSRVR "149.12.34.567"
SET ACTIVE_CSDK_BASED_PHONE_APP "com.avaya.android.flare"
SET TRUSTCERTS "prod-sip-ca.crt,digi-intermed.txt"
SET SIP_CONTROLLER_LIST "135.12.345.670:5061;transport=tls"
SET SIPDOMAIN "avaya.com"
SET USER_AUTH_FILE_SERVER_URL "https://aads.service.com:8443"
SET TLSSRVRID 0
```

The double quotes (“”) are optional for the above configuration parameter examples. However, to include spaces in a parameter value, you must enclose the value using double quotes (“”)

Some considerations while configuring parameters:

- When you are using user enterprise credentials for authentication through Avaya Aura® Device Services, you must configure USER_AUTH_FILE_SERVER_URL.
- Although Avaya Aura® Device Services identity certificate root CA is available in the Android “VPN and APPS” trusted certificate repository, you must include it in the downloaded trusted certificates defined in TRUSTCERTS.
- You must configure SNTPSRVR if the default Avaya and NIST SNTP servers are not accessible from the customer network. Specifying an SNTPSRVR value that is reachable from your network is essential for SIP registration and initial device setup when you start up Avaya Vantage™.

Parameter configuration example for IP Office with SIP credentials

The following is an example of mandatory parameters included in the automatically generated settings file for an IP Office deployment with SIP credentials:

```
SET SNTPSRVR "149.12.34.567"
SET TRUSTCERTS "prod-sip-ca.crt"
SET SIP_CONTROLLER_LIST "135.12.345.670:5061;transport=tls"
SET SIPDOMAIN "avaya.com"
SET TLSSRVRID 1
SET ENABLE_IPOFFICE 1
SET SUBSCRIBE_LIST_NON_AVAYA "reg, message-summary, avaya-ccs-profile"
SET UPGRADE_POLICY 0
SET SIMULTANEOUS_REGISTRATIONS 1
SET POUND_KEY_AS_CALL_TRIGGER 0
```

The double quotes (“”) are optional for the above configuration parameter examples. However, to include spaces in a parameter value, you must enclose the value using double quotes (“”)

Some points to consider for device configuration in the IP Office environment:

- The TIMEZONE and ACTIVE_CSDK_BASED_PHONE_APP parameters are not part of the automatically generated configuration file. ACTIVE_CSDK_BASED_PHONE_APP is part of the automatically generated upgrade file. You can configure TIMEZONE and additional parameters separately in the `46xxspecials.txt` file. You can also override parameters in the automatically generated configuration file using the `46xxspecials.txt` file.
- USER_AUTH_FILE_SERVER_URL must remain with the default value, which is null (“”).
- TLSSRVRID is set to 0 if:
  - The identity certificate of Avaya Vantage™ services does not include Subject Alternative name with the FQDN or IP address of the services.
  - The SIP controller identity certificate does not include the correct SIP domain in Subject Alternative Name.
  - The identity certificate does not include a common name field for other services.
- UPGRADE_POLICY is set to 0 because IP Office uses the push method for software upgrades instead of automatic polling for upgrade files by the device.

Index

Special Characters

_REPLACE THIS TEXT, OR DELETE THIS ENTIRE INDEXTERM ELEMENT IF YOU DO NOT NEED IT 180

Numerics

802.1X
- pass through 124
- supplicant 124

A

AADS server configuration 24
accessibility parameters 311
access to Google Play 132
activating administrator settings 118
active CSDK application setting 131
ADB 80
- enabling or disabling through the Settings menu 80

adding feature buttons
- in Avaya Aura environment 157
- in IP Office 159

administering device
- 802.1X 124
- Ethernet interface control 123

administration methods 100
administrator mode 118
administrator password 70
Android application package names
- how to find 190

Android Debug Bridge 80
Android installation wizard 50
application download control
- XML file 133

application installation 127
- CSDK-based application package names 132
- push application 128
- setting up active telephony application 130

application installation policy 134
application package names 132
applications
- parameters 244
- uninstalling pushed applications 129

audio parameters for client SDK application 246
audio report
- decrypting 168
- generating 166

autodial 149
automatic firmware upgrade 29
automatic upgrade 177
Avaya Aura configuration 23
Avaya Aura Device Services for device configuration 115
Avaya Breeze Client SDK parameters 246
Avaya certificate generation in DES 30
Avaya Connect Expansion Module
- configuration 153
- parameters 261

Avaya CSDK-based applications
- package names 132

Avaya product certificate 77
Avaya SIP Product CA certificate 77
Avaya support website 195
Avaya telephony applications 130
Avaya Vantage
- connecting to the network 49
- wall mounting 57, 58
- wall mounting on a wall plate 59
- wall mounting with handset cradle 62

Avaya Vantage connect
- feature configuration 149

Avaya Vantage Connect
- Exchange Calendar configuration 152

Avaya Vantage Connect parameters
- audio codec 261
- calendar 261
- companion application 261
- Expansion Module 261
- hot dialing 261
- logo setting 261

Avaya Vantage overview 16

B

best practices
- security 67

black list 133, 134

C

calendar configuration parameters 152
call pickup 158
captive portal 280
certificate
- self-signed 76

certificate error on the device 187
certificates 73
- management 71

certificates configuration parameters 281
checklist
- device configuration 116
- Expansion Module setup 155
- hot dialing configuration 149
- installation 20
- kiosk mode configuration 141

clear user data in PPM 162

Client SDK parameters
audio ... 246
conferencing ... 246
contact management ... 246
dial plan ... 246
logging ... 246
RTP ... 246
SRTP ... 246
video ... 246
codec parameters ... 246
collection
delete ... 193
edit name ... 193
generating PDF ... 193
sharing content ... 193
comparison
Avaya Aura vs IP Office ... 26
conditional statements in the settings file ... 112
conferencing parameter for client SDK application ... 246
configuration
emergency call ... 136
configuration data
Avaya Aura Device Services ... 115
configuration priority
CSDK-based telephony application ... 101
configuration verifier ... 125
configuring device
using DHCP ... 106
using LLDP ... 101
configuring parameters ... 39, 115
configuring SSH server settings ... 169
configuring the log settings ... 163
configuring Wi-Fi ... 53
Connect application
user information ... 96
connecting
handset cradle ... 54
wired handset ... 55
wireless handset ... 56
connecting Avaya Vantage to the network ... 49
connectivity ... 48
considerations
installation wizard ... 50
contact comparison ... 138
contact functionality ... 138
contact parameters for client SDK application ... 246
contacts
Avaya Aura Device Services ... 139
PPM ... 139
contact search
IP Office ... 139
content
publishing PDF output ... 193
searching ... 193
sharing ... 193
watching for updates ... 193
copying log from internal flash memory ... 168
corrupt firmware ... 184
corrupt system file ... 184
CSDK application upgrades ... 183
CSDK-based applications
package names ... 132
customization of settings file ... 112

D

dark boot up ... 145
data categories
personal data ... 91, 95
data privacy controls ... 90
debugging options ... 163
debug report
copying from internal flash memory ... 168
generating ... 164
opening ... 168
decrypting
debug report ... 168
deployment comparison ... 26
deployment through Device Enrollment Services ... 30
DES_STAT ... 30
DES discovery ... 30, 49
Device
user information ... 91
device configuration ... 100
screen saver ... 146
verifying ... 125
device configuration checklist ... 116
device connectivity ... 48
device enrollment firmware ... 29
Device Enrollment Services ... 30, 78
Avaya certificate generation ... 30
secure redirection to provisioning server ... 29
Device Enrollment Services firmware upgrades ... 29
device lock parameters ... 294
device settings
DNS configuration ... 119
file server address ... 119
device setup using installation wizard ... 50
device upgrade ... 172
DHCP
option 43 codes ... 107
options configuration ... 106
parameter configuration ... 108
setting up a DHCP server ... 36
site-specific parameters ... 109
vendor-specific option ... 107
DHCP server setup ... 36
DHCP settings worksheet ... 32
DHCP site-specific option number ... 123
diagnostics ... 163
SLA Mon ... 171
dial plan parameters for client SDK application ... 246
directory search ... 138
LDAP ... 139

DNS configuration
configuration through settings menu 119
documentation portal 193
finding content 193
navigation 193
document changes 12
downloading the firmware 39
duplex setting
Ethernet interface 123

E

EASG site certificate 281
editing black or white list 134
emergency call configuration 136
parameters 136
emergency call settings
parameters 298
ENABLE_CORDLESS_HANDSET_UPDATE parameter .. 183
enabling administrator settings 118
enabling port mirroring 170
enabling syslog 163
erasing user information from PPM 162
Ethernet interface control
duplex and speed 123
Ethernet interface settings 236
example
parameter configuration for Avaya Aura with SIP credentials 313
parameter configuration for Avaya Aura with user enterprise credentials 314
parameter configuration for hot dialing 151
parameter configuration for IP Office with SIP credentials 314
Exchange server configuration
Avaya Vantage Connect 152
exiting the kiosk mode 144
Expansion Module
adding feature buttons 157
configuration 153
configuration checklist 155
supported feature buttons 154
extracting
Avaya SIP Product CA certificate 77
System Manager CA certificate 78

F

Failover and survivability 163
feature button
adding in Avaya Aura environment 157
adding in IP Office 159
feature configuration
Avaya Vantage Connect 149
file server
setting up 38
file server address
file server address *(continued)*
configuring through Settings menu 119
file server configuration 36
parameters 213
finding Android application package name 190
finding content on documentation portal 193
FIPS mode 83
configuration 84
disabling from the Settings menu 85
parameter 289
firmware 29
downloading 39
firmware got corrupted 184
firmware upgrade 172
firmware upgrade prerequisites 173
full VLAN separation 81

G

generating PKCS12 file 75
generating report
audio 166
debug 164
Google Play Store
access control 132
editing black or white list 134
Goto command in the settings file 112

H

H.323 contacts
no phone number 188
handset
connecting 54, 55
wireless 56, 57
handset cradle
connecting to the device 54
hardware requirements 21
host pinging 170
hot dialing 149
configuration checklist 149
parameter configuration example 151
parameters 261
HTTP proxy settings 121
HTTPS file server
self-signed certificate 76

I

idle time configuration 148
idle time parameters 294
IEEE 802.1.x settings 241
InSite Knowledge Base 195
install applications 127
CSDK-based application package names 132
installation checklist 20

installation wizard 50
installing a wireless module 52
IP address configuration 41
IP interface
    IPv4 configuration 47
    IPv6 configuration 47
IP Office
    conference access code 190
    user settings 32
IP Office configuration 25
IP Office contact search 139
IPv4 and IPv6 support
    overview 41
IPv4 configuration
    Settings menu 47
IPv6 configuration
    Settings menu 47
IPv6 operation
    configuration parameters 42
IPv6 support 41

K

K155 wireless module 52
K165
    setting up using installation wizard 50
K175
    setting up using installation wizard 50
kiosk mode 141
    application packages 142
    application pinning 142
    configuration checklist 141
    existing 144
    quick lock 142
    starting 143
Kiosk mode
    unpinning applications 143

L

LDAP directory search 139
LDAP directory service
    parameters 308
LLDP
    content transmitting in LLDP frames 102
    overview 101
    TLV impact on system parameter values 103
local log configuration 163
lock parameters in Settings 296
lock parameters in Settings menu 82
lock screen behavior 148
logging parameters for client SDK application 246
Login screen behavior 145
login screen settings 293
login settings 145
log reports 163
logs
logs *(continued)*
    clear local logs 163

M

manual reboot 162
Microsoft Exchange server
    Avaya Vantage Connect 152
monitoring options 163
My Docs 193

N

network
    user information 91, 96
network connection 48, 49
network parameters 226
    Ethernet settings 236
    general settings 227
    IEEE 802.1.x settings 241
    VLAN settings 238
new in this release 17
non UI related operational parameters
    active phone application 243
    LDAP directory service 308
    server addresses and ports 213
    server environment 225
    SLA Mon agent 306
NTP configuration 40
numeric enrollment code 49

O

obscure parameters in Settings 296
obscure parameters in Settings menu 82
online help URL 312
opening
    debug report 168
option 43 codes 107
optional components 16
overview 16

P

pairing wireless handset 56
parameter configuration 39, 115
parameters
    accessibility 311
    application settings 244
    Avaya Breeze Client SDK 246
    Avaya Vantage Connect parameters 261
    calendar integration 152
    certificates settings 281
    device lock 294
    device UI related settings 201
    emergency numbers 136, 298

parameters *(continued)*
Expansion Module 261
file server configuration 213
FIPS mode 289
general accounts IDs & passwords 289
general phone functionality 198
hot dialing 261
IP Office parameters 272
IPv6 operation 42
lock preferences 296
logging and debugging 300
login screen behavior 293
network parameters 226
obscure preferences 296
online help URL 312
parameters for controlling configuration parameter download 196
phone specific parameters 197
protocol-specific parameters 280
screen saver configuration 146
SELinux 288
SIP proxy configuration 213
SIP registrar configuration 213
SIP user credential settings 224
upgrade-related parameters 174, 275
VLAN configuration 81
password security policies 69
patches
Android 86
performing a scheduled upgrade 177
personal data
Avaya Vantage
export controls 94
programmatic or API access controls 93
pseudonymization 95, 99
retention period controls 94
Avaya Vantage Connect
export controls 99
programmatic or API access controls 97
pseudonymization 95, 99
retention periods 98
human access controls 92, 96
personal data at rest
Avaya Vantage
encryption controls 93
Avaya Vantage Connect
encryption controls 97
personal data in transit
Avaya Vantage
encryption controls 93
Avaya Vantage Connect
encryption controls 98
PIN_APP
package names 142
pin applications
package names 142
pinging a device on the network 170
pinning in Kiosk mode 142
PKCS12 file
adding friendly name 76
certificate with friendly name 75
PKCS12 parameters 281
Platform
user information 91
port mirroring
enabling 170
power 48
power outage during upgrade 184
power sources 48
PPM 23
clear user data 162
H.323 contacts 188
prerequisites 21
firmware upgrade 173
priority
CSDK-based telephony application 101
protocol-specific parameters
LLDP 280
TLS 280
push applications 127
push applications onto device 128
examples 129

Q

quick lock for kiosk mode 142

R

reboot 162
recovery procedure 184
related documentation 191
remote logging 163
removing paired wireless handset 57
requirements
hardware 21
software 21
reset a device to factory settings 161
RFC 2833 190
ring down 149
RTP parameters for Client SDK application 246

S

SAL Mon agent
parameters 306
scenario
automatic upgrade 177
scheduled upgrade 177
SCEP parameters 281
scheduled upgrade 177
screen saver configuration 146
screen saver configuration parameters 146

searching for content 193
secure installation
parameters 86
secure redirection through DES 29, 78
security
secure redirection through DES 78
SSH access control 79
time synchronization 79
user privacy 68
security configuration 65
security features 65
security patches 86
security recommendations 67
self-signed certificate
recommendations 76
sending user information over the network 91, 96
server
setting up a DHCP server 36
server configuration
AADS 24
System Manager 23
server environment
parameters 225
server setup
DHCP 36
file server 36
Session Border ControllerSIP user agent
configuring 28
settings file 111
conditional statement 112
configuring parameters 39, 115
customization 112
Goto command 112
user group 112
worksheet 33
settings file structure 112
Settings menu
administrator mode 118
lock parameters 82
obscure parameters 82
Settings menu options
obscure or lock 82
Settings screen
AADS configuration 120
HTTP proxy and exception 121
SIP server 122
setting up active telephony application 130
setting up a DHCP server 36
sharing content 193
silent boot up 145
SIP Product CA certificate 77
SIP proxy configuration
parameters 213
SIP server settings 122
SIP user credential settings
parameters 224
SIP user settings
SIP user settings *(continued)*
IP Office 32
site-specific options
list of parameters 109
SLAAC
enable through Settings menu 47
SLA Mon agent 171
sleep time settings 148
SNTP server 79
SNTP server setup 40
software download 39
software requirements 21
SSH access control 79
SSH server
configuring settings 169
starting Avaya Vantage 49
starting kiosk mode 143
start-up configuration
dark and silent start-up 145
static IPv4 address configuration 47
static IPv6 address configuration 47
storage
user information 91, 96
support 195
syslog
configuring remote logging 163
syslog configuration 163
System Manager CA certificate 78
System Manager configuration 23
System Manager user profile worksheet 31

T

talkback 311
telephony application
configuration priority 101
third-party applications 133
third-party application stores 133
time synchronization 40, 79
TLV impact on system parameter values 103
training 194
troubleshooting 184
access code for meet-me conference 190
applications not downgrading on K175 189
applications not supported on Android 8.1 188
Avaya IX Workplace Client not downgrading 189
call stuck 189
cannot call H.323 contacts 188
cannot dial access code 190
cannot find application package names 190
conference 190
device does not dial access code 190
downgrade from Android 8.1 to Android 6.x 188
DTMF 190
forceUnauthorized 189
H.323 contacts downloaded from PPM without a phone number 188

troubleshooting *(continued)*
in-band DTMF 190
IP Office conference access code 190
no prompt for password to unlock 186
no video 186
port switch change 189
security certificate error 187
software packages cannot be uploaded using Utility Server 185
software zip files too large 185
swipe to unlock does not prompt for password 186
TRUSTCERTS configuration 187
Utility Server file size 185
video is not enabled 186
video remains stuck 186
video setting in Communication Manager 186
TRUSTCERTS 281
TRUSTCERTS configuration 187
Two different directories 180
Two different file servers 180

U

uninstall pushed applications 129
unknown sources 133
unpairing wireless handset 57
unpin applications 143
updates
CSDK applications 183
upgrade 172
automatic 177
procedure 172
using Update Now option 178
upgrade policy parameters 174
upgrade prerequisites 173
upgrade wireless handset
enabling through the settings file 183
upgrading
through IP Office 179
through System Manager 178
uploading software zip file to Utility Server 185
USB parameters 307
use of self-signed certificate
recommendations 76
user agent configuration 28
user group 112, 121
configure using settings file 114
user information storage 91
Avaya Vantage Connect 96
user profile 31

V

Vantage device
user information 91
vendor-specific DHCP option 107
verifying configuration 125
video device configuration 24
video parameters for client SDK application 246
videos 194
VLAN configuration parameters 81
VLAN separation 81
VLAN settings 238

W

wall mounting 57
on a phone wall plate 59
with handset cradle 62
with screws 58
watch list 193
white list 133, 134
Wi-Fi network configuration 53
wired handset
connecting 55
wireless handset
enabling upgrade 183
pairing 56
remove pairing 57
wireless module 52
worksheets
DHCP settings worksheet 32
settings file worksheet 33
System Manager user profile worksheet 31

X

XML file for application control 133