



Installing and Administering Avaya VantageTM

Release 1.0
Issue 3
November 2017

Note

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE

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

Japan Statements

Class B Statement

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

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

取扱説明書に従って正しい取り扱いをして下さい。 VCCI-B

Denan Power Cord Statement



Danger:

Please be careful of the following while installing the equipment:

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

guidelines are not followed, it may lead to death or severe injury.



警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

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

México Statement

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

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

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

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

Power over Ethernet (PoE) Statement

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

U.S. Federal Communications Commission (FCC) Statements

Compliance Statement

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

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

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

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

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

Class B Part 15 Statement

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

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designated to provide reasonable protection against harmful interferences in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interferences to radio or

television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Radiation Exposure Statement

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

EU Countries

This device complies with the essential requirements and other relevant provisions of Radio Equipment Directive 2014/53/EU. A copy of the Declaration may be obtained from <http://support.avaya.com> or Avaya Inc., 4655 Great America Parkway, Santa Clara, CA 95054–1233 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.

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

Contents

Chapter 1: Introduction	9
Purpose	9
Change history	9
Chapter 2: Avaya Vantage™ overview	11
Physical device layout	11
Connectors and controls	12
Optional components for the Avaya Vantage™ device	14
Wireless handset layout	15
Chapter 3: Initial setup and connectivity	16
Initial setup checklist	16
Software and hardware prerequisites	16
Preinstallation data	17
Specifications	19
Connecting a handset to Avaya Vantage™	23
Connecting the handset cradle to Avaya Vantage™	23
Connecting a wired handset	24
Connecting a wireless handset	24
Power management	26
Connecting Avaya Vantage™ to the network	26
Chapter 4: Server, device, and security configuration	28
Server configuration	28
Server configuration checklist	28
DHCP server configuration	29
File server configuration	29
Avaya Session Border Controller for Enterprise configuration	30
Avaya Aura® System Manager configuration	31
PPM configuration	31
Avaya Aura® Device Services configuration	32
Device configuration	32
Device configuration using DHCP options	33
Device configuration using a 46xxsettings.txt settings file	37
Device configuration using LLDP	40
Device configuration using the Settings menu on the device	43
Security configuration	48
Password security policies	50
Certificate management	50
Certificate usage by applications	51
Configuring security parameters	52
Chapter 5: Application setup	55

Pushing applications onto the Avaya Vantage™ device.....	55
Push command examples.....	56
Uninstalling a pushed application.....	56
Administering access to Google Play applications.....	57
Editing black and white lists.....	57
Setting up a CSDK-based telephony application as the active application.....	58
Avaya telephony applications supported on Avaya Vantage™	59
Package names of CSDK-based applications.....	59
Chapter 6: Maintenance	60
Device upgrade.....	60
Device upgrade process.....	60
Automatic upgrade.....	61
Upgrading Avaya Vantage™ using System Manager.....	61
Upgrading Avaya Vantage™ using the Update option.....	62
Restoring factory settings.....	62
Rebooting Avaya Vantage™	63
Failover and survivability.....	63
Debugging and monitoring the device.....	63
Enabling verbose logging.....	63
Generating a debug report.....	64
Opening a debug report.....	65
Pinging a device on the network.....	65
Chapter 7: Troubleshooting	66
Firmware is corrupted.....	66
Chapter 8: Resources	68
Documentation.....	68
Finding documents on the Avaya Support website.....	69
Viewing Avaya Mentor videos.....	70
Support.....	70
Using the Avaya InSite Knowledge Base.....	70
Appendix A: Supported configuration parameters	72
Parameters for controlling configuration parameter downloads.....	72
Phone parameters.....	73
General phone functionality.....	73
Phone UI related settings.....	74
Network settings.....	82
General settings.....	82
Ethernet interface settings.....	89
VLAN settings.....	89
IEEE 802.1X settings.....	91
Server addresses and ports.....	92
Other operational parameters and settings.....	100
Active phone application.....	101

Third party applications..... 101

Dial plan parameters..... 103

Protocol-specific parameters..... 103

Logging and debugging parameters..... 111

USB parameters..... 114

Upgrade related parameters..... 115

General account IDs & passwords..... 118

Phone lock parameters..... 120

Security parameters..... 122

Avaya Breeze™ CSDK parameters..... 122

Avaya Vantage™ Basic parameters..... 129

Appendix B: Unsupported configuration parameters..... 134

Chapter 1: Introduction

Purpose

This document provides checklists and procedures for installing, configuring, administering, and troubleshooting Avaya Vantage™. This document is primarily intended for implementation engineers and administrators.

Change history

Issue	Date	Summary of changes
Release 1.0 (Controlled Introduction GA), Issue 1	March 2017	This is a new document that is being issued for the first time in this release.
Release 1.0 (Unrestricted GA), Issue 2	June 2017	• Updated information about package components in Optional components for the Avaya Vantage device on page 14. • Added a warning about the 3.5 mm phone connector in Specifications on page 19. • Described wireless handset support specifications and features. • Removed information about USB charging. • Added additional steps in Connecting the handset cradle to Avaya Vantage on page 23. • Added wireless handset setup information in Connecting a wireless handset on page 24. • Added wireless handset information in Wireless handset specifications on page 20 and Wireless handset features on page 21. • Added a description of Avaya Vantage™ operational modes in Device configuration on page 32. • Moved information about service, device, and security configuration into a separate chapter, and restructured the information in this chapter.

Table continues...

Issue	Date	Summary of changes
		• Updated application setup information and moved the content into a separate chapter. • Updated information about the Recovery screen navigation in Firmware is corrupted on page 66. • Updated the information about supported configuration parameters in Appendix A.
Release 1.0, Issue 3	November 2017	Updated the Legal content with a statement about the Radio Equipment Directive in EU countries..

Chapter 2: Avaya Vantage™ overview

Avaya Vantage™ is an Android™ device that provides telephony and conferencing functionality. Avaya Vantage™ combines the advantages of a customizable unified communications solution and a fully functional Android device. Use Avaya Breeze™ Client Software Development Kit and custom applications to integrate communications in business processes on your Avaya Vantage™ device.

According to your business needs, you can choose one of the following Avaya Vantage™ devices:

- Avaya Vantage™ with an integrated camera if you need full access to video calls and conferences. You can cover the camera using the mechanical camera shutter.
- Avaya Vantage™ without an integrated camera and privacy shutter. You can still receive video from other devices.

Physical device layout

Avaya Vantage™ resembles a tablet in portrait orientation. The device also includes volume control buttons. Avaya Vantage™ with an integrated camera also includes a camera privacy shutter.

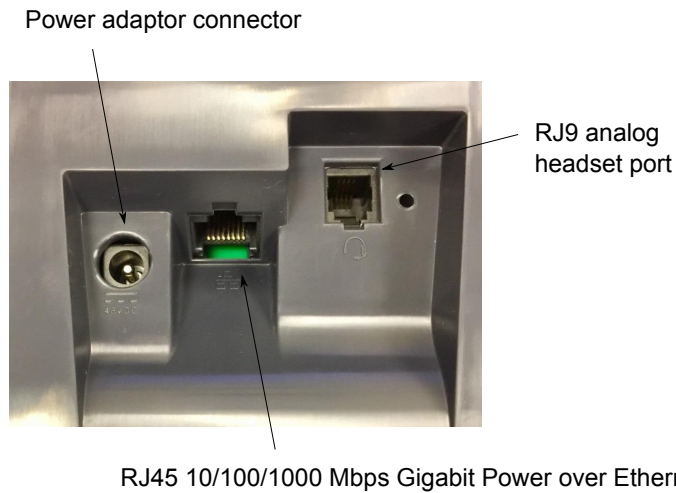


Connectors and controls

The following images show the options available on the Avaya Vantage™ device.

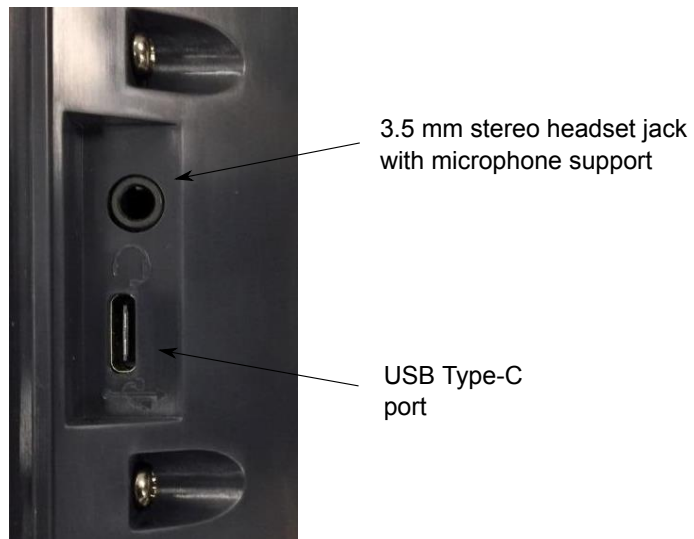
Rear panel

The rear panel contains a power adaptor connector, an RJ9 headset port, and an Ethernet port.



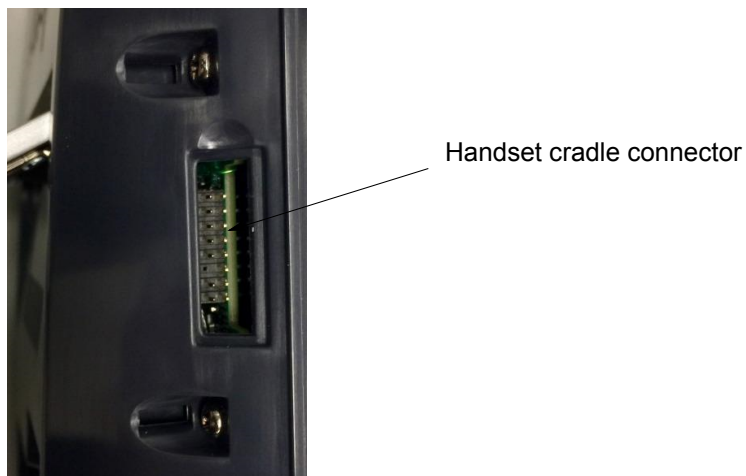
Right side panel

The right side panel contains a 3.5 mm audio jack socket and a USB Type-C port.



Left side panel

The left side panel contains a cordless or corded handset cradle connector.



Handset cradle connector

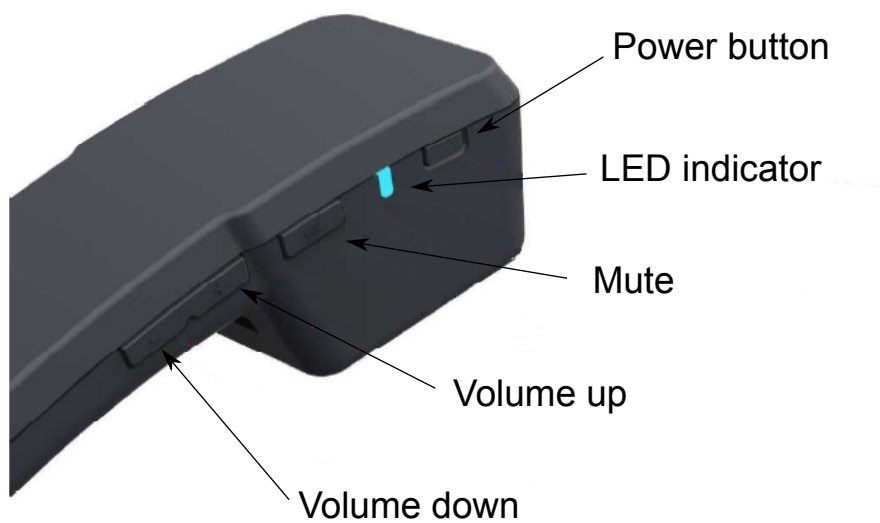
Optional components for the Avaya Vantage™ device

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

- Wired or wireless handset and cradle kit
- Replacement handset cord
- AC power adaptor (international)
- AC power cord for regions

Optional components are packaged separately.

Wireless handset layout



Chapter 3: Initial setup and connectivity

Initial setup checklist

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

No.	Task	Notes	✓
1.	Review prerequisite information.	If you do not have all required software and hardware, Avaya Vantage™ might not function as expected.	
2.	Gather preinstallation data.	Preinstallation data is required to perform initial parameter setup and to create user accounts for Avaya Vantage™.	
3.	Ensure that the Avaya Vantage™ package contains all required components	See Optional components for the Avaya Vantage device on page 14.	
4.	Connect a handset.	This is an optional task. Perform this task if you want to use a handset with Avaya Vantage™.	
5.	Connect Avaya Vantage™ to a power supply and to your network.		

Software and hardware prerequisites

Check the following prerequisites before you install Avaya Vantage™.

Components and other software prerequisites

The following components must be installed and configured in your network:

- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® System Manager
- Avaya Aura® Presence Services
- Avaya Aura® Session Border Controller
- Avaya Aura® Device Services

- A DHCP server for providing dynamic IP addresses
- A file server, an HTTP, HTTPS, or the Avaya Aura® Utility Services for downloading software distribution packages and the settings file
- One or both of the following conference servers for audio and video conference:
 - Avaya Aura® Conferencing
 - Scopia Elite MCU

Avaya Vantage™ requires Avaya Aura® Release 7.0.1.2. For detailed information about supported product releases, see the [Avaya Compatibility Matrix](#).

Hardware connection prerequisites

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 the AC power adaptor, which can be ordered with the device.

Related links

[Specifications](#) on page 19

Preinstallation data

System Manager user profile worksheet

To create a user profile on System Manager for Avaya Vantage™ Basic or Avaya Equinox™, 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

Table continues...

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

Settings file worksheet

In the following table, populate the following values for your deployment:

Parameter	Your value
SIP_CONTROLLER_LIST	
SIPDOMAIN	
ACTIVE_CSDK_BASED_PHONE_APP	
SNTPSRVR	
FILE_SERVER_URL	
USER_INSTALL_APPS_GOOGLE_PLAY_STORE	
TRUSTCERTS	

Table continues...

Parameter	Your value
ADMIN_PASSWORD or PROCPSWD	
ISO_SYSTEM_LANGUAGE	
TIMEFORMAT	
TIMEZONE	
COUNTRY	

*** Note:**

Avaya Vantage™ Basic and Avaya Equinox™ are the only Avaya Breeze™ Client Software Development Kit applications supported in the current release.

DHCP settings worksheet

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

Option or parameter	Your value
Range of IP addresses	
DHCP options	
FILE_SERVER_URL	
HTTPSRVR	
TLSSVR	

*** Note:**

If the FILE_SERVER_URL parameter is defined, Avaya Vantage™ ignores HTTPSRVR and TLSSVR.

Specifications

Specification	Supported on Avaya Vantage™
Screen	• Capacitive touch screen. • Resolution: 1280×800 px. • 24 bits color depth.
Headphone Out	• 3.5 mm phone connector.  Warning: Avoid listening at a high volume with devices that are connected to the 3.5 mm connector to prevent hearing damage. • RJ9 headset connector for a high quality wired headset.

Table continues...

Specification	Supported on Avaya Vantage™
USB port	x1 USB 2.0 Type-C general purpose port.
Internal storage	16 GB flash memory.
Power	• Power over Ethernet IEEE 802.3af (Class 3) or 802.3at (Class 4). • Dedicated 48Vdc power supply. Use Delta Electronics Inc. model ADP-30HR B, output 48Vdc, 0.66A.
Operating system	Android 6.0.1 (Marshmallow).
Ethernet	RJ45 primary Gigabit Ethernet (10/100/1000 Mbps) PoE LAN port.
Wi-Fi	• Wireless access point mode. • Wi-Fi 802.11a/b/g/n/ac.
Bluetooth	Bluetooth 4.2 supporting High Speed (HS), Low Energy (LE), and Enhanced Data Rate (EDR) functionality.
Supported Bluetooth profiles	• Advanced Audio Distribution Profile (A2DP). • Headset Profile (HSP). • Human Interface Device Profile (HID). • Object Push Profile (OPP).
Supported Accessories	• 3.5 mm headset. • RJ9 headset. • Bluetooth headset. • USB pen drive.
Audio	Supported codecs: • G.722 • G.711 • G.729 • G.726 • Opus
Physical security	Kensington security slot.
Stand	A stand that can be used either as a desk stand or a wall-mount stand. The stand supports a standard 100mm pin spacing Ethernet wall plate.

Related links

[Software and hardware prerequisites](#) on page 16

[Wireless handset specifications](#) on page 20

Wireless handset specifications

Specification	Avaya Vantage™ wireless handset
System	Bluetooth 4.1

Table continues...

Specification	Avaya Vantage™ wireless handset
Profiles	• Hands-free Profile 1.6. • Headset Profile.
Battery	0.56 W, 3.7 V Li-Ion battery.
Battery charger	Li-Ion battery management system.
Charging system	Contactless charging system: inductive coupling to the cradle.
Controls	• Power button. • Mute button. • Volume up button. • Volume down button.
Indicators	Blue LED indicator.
Operating environment temperature	0 to 49 °C (32 to 120 °F).
Battery charging environment temperature	0 to 40 °C (32 to 104 °F).
Weight	170 grams.

Wireless handset features

Range

The handset uses Bluetooth technology. As a Class 2 device, the handset nominal range is 10 meters. In practical use this range might vary depending on the environment. If the handset was out of range, the connection is reestablished automatically when the handset is back in range. When the handset is not in range for more than 22 minutes, it turns off to prevent battery discharge. If the handset was turned off, the connection is reestablished automatically when the handset is turned on and back in range.

Battery service life

If used carefully, the expected service life of the battery is several years. Although the battery capacity is diminished over time, in general it does not affect normal handset use.

Battery talk time

When fully charged, the new battery provides approximately 12 hours of talk time. You might need to charge the battery before the first use to achieve the full talk time. To prevent damage to the battery, the protection system does not allow the battery to discharge below a certain point. Avaya Vantage™ displays the battery charge level on the Notifications panel.

Battery standby time

When fully charged, the new battery provides approximately 60 hours of standby time. When the handset is not in range or Avaya Vantage™ is turned off for approximately 22 minutes, the handset is turned off automatically to save battery. To turn on the handset again, press the **Power** button for approximately 2 seconds. The handset is not turned on automatically even if it is returned to the cradle.

Battery charging

The handset supports a contactless charging system. To charge the handset, place it in its cradle. If the battery charge is low, the handset will notify you with warning tones. When you hear the warning tones, return the handset to its cradle to charge the battery.

The handset uses a Lithium-Ion battery with the battery management and protection system. The protection system allows to prevent the following situations:

- Overcharging.
- Over-discharging.
- Charging if the ambient temperature is higher than 40 °C (102 °F).

Battery recharge time

The battery fully recharges in less than 3 hours. You do not need to fully discharge the battery before charging.

Battery disposal

At the end of the service life, remove the battery and deliver it to a battery recycling depot. Do not dispose of the battery in the normal waste stream.

Wireless handset LED indicator

The blue LED indicator shows the current state of the handset and is also used to indicate user actions.

Wireless handset state	LED indication	Notes
Wireless handset is in the Pairing mode.	LED flashes every 0.5 seconds.	Wireless handset exits the Pairing mode in 150 seconds.
Pairing completed successfully.	LED flashes 10 times at 0.1 seconds rate.	None
Wireless handset is used in a call	LED flashes 3 times every 3 seconds	None
Wireless handset is turned on and is connected to its base (Connected mode).	LED flashes 2 times every 5 seconds.	None
Wireless handset is trying to establish connection to its base (Linkback mode).	LED flashes every 0.5 seconds.	None
Wireless handset is out of range and is not trying to establish connection to its base (Standby mode).	LED flashes every 5 seconds.	Wireless handset is turned off after 22 minutes.
Incoming call.	LED flashes 3 times every 7 seconds.	None
Mute.	LED is on and flashes 3 times every 4 seconds.	None

Table continues...

Wireless handset state	LED indication	Notes
Wireless handset has been turned on.	LED flashes 4 times.	None
Wireless handset has been turned off.	LED flashes 3 times.	None

Power button

The **Power** button provides the following functionality:

Action	How to use	Handset LED confirmation
Turn on the handset	Press and hold the button for 2.4 seconds	LED flashes 4 times
Turn off the handset	Press and hold the button for 3.2 seconds	LED flashes 3 times
Enable pairing mode	Press and hold the button for 10 seconds	LED flashes at 0.5 seconds rate

Connecting a handset 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. To use a handset with Avaya Vantage™, you also need to connect a handset cradle.

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.

Note:

Be careful when installing the cradle to avoid bending 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

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. From the left side of the Avaya Vantage™ device, remove the rubber gasket that protects the cradle connector pins.
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. 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 to your Avaya Vantage™ device. You cannot use the wired handset if you connect the wireless handset. You can connect only one wireless handset at a time.

Before you begin

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

Procedure

1. Lift the wireless handset from the cradle, and press and hold the top button until the LED starts flashing.



2. From the Home screen, tap **Applications**.
3. Tap **Settings**.
4. Tap **Bluetooth**.
You might need to enter the administrator password to view the **Bluetooth** menu on the Settings screen.
5. Turn Bluetooth on.
6. In the list of available devices, tap the entry that matches the ID on the handset label.

If pairing is successful, Avaya Vantage™ displays the wireless handset in the list of paired devices as connected.

Result

You can now 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 to Avaya Vantage™. When you turn on the handset, you do not need to repeat the pairing procedure.

Power management

Avaya Vantage™ receives power from the following sources:

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

If your network does not support the 802.3af or 802.3at PoE specification, you can use a 48 Volt, 30 Watt power adaptor to power Avaya Vantage™. You can purchase the power adaptor separately.

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

- If the power adaptor is disconnected, Avaya Vantage™ reboots. If the networking switch supports either the 802.3at or 802.3af specification, Avaya Vantage™ continues to work after the reboot.
- If the networking switch is disconnected, Avaya Vantage™ continues to work without a reboot.

If Avaya Vantage™ is connected to the PoE networking switch and the power adaptor is connected, Avaya Vantage™ continues to work without a reboot.

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

Connecting Avaya Vantage™ to the network

About this task

You can connect Avaya Vantage™ to your network using a wireless or Ethernet connection.

Procedure

1. To use a wired Ethernet connection:
 - a. Plug one end of an Ethernet cable into the LAN connector at the back of Avaya Vantage™.
 - b. Plug the other end of the Ethernet cable into an available LAN port in your network.

2. To use a Wi-Fi connection:
 - a. From the Home screen, tap **Applications**.
 - b. Tap **Settings**.
 - c. Tap **Network > Network mode**.
 - d. Select **Wi-Fi**.
 - e. In the Network screen, tap **Wi-Fi** and choose a required network.
 - f. **(Optional)** Enter network credentials, if prompted.

If you are using a wireless connection, you must connect Avaya Vantage™ to a power source.

3. If your network does not support the 802.3at (PoE+) or 802.3af (PoE) injector specification, connect the power adaptor to the 48-V DC power connector and plug the power adapter into an electrical outlet.

Chapter 4: Server, device, and security configuration

Server configuration

To install Avaya Vantage™, you must configure the following servers:

- DHCP server: To dynamically assign IP addresses and provide device configuration parameters.
- HTTP or HTTPS server: To download and save the software distribution package and the `46xxsettings.txt` settings file.

To use Avaya telephony applications or to use Avaya Vantage™ in Avaya environment, you can also configure the following servers:

- Avaya Aura® System Manager: To create users for Avaya telephony applications, such as Avaya Equinox™ and Avaya Vantage™ Basic 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.
- Avaya Session Border Controller for Enterprise (Avaya SBCE): To use Avaya Vantage™ devices in networks controlled by Avaya SBCE.

Server configuration checklist

The following checklist describes tasks that you must perform to configure Avaya Vantage™ service settings.

No.	Task	Notes	✓
1.	Ensure that you have all required licenses for the DHCP and file server software.	Contact your server software vendors to obtain information about server licensing.	
2.	Ensure that a DHCP server is installed and configured.	Contact your DHCP server vendor to obtain installation documentation. For configuration information, see DHCP server configuration on page 29.	

Table continues...

No.	Task	Notes	✓
3.	Ensure that a file server is installed and configured.	Contact your file server vendor to receive installation documentation. For configuration information, see File server configuration on page 29.	

DHCP server configuration

Configure the DHCP server to:

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

Setting up a DHCP server

Procedure

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

Avaya Vantage™ supports any DHCP server software as long as the software is correctly configured. Contact your server software vendor to obtain server software installation and configuration instructions.

2. Configure the available range of IP addresses.
3. Configure the required DHCP options.

File server configuration

A file server is an HTTP or HTTPS server that is used for downloading and storing software distribution packages, setting files, 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.

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

- DHCP
- LLDP
- The **Settings** menu on the Avaya Vantage™ device
- `46xxsettings.txt` settings file

For LLDP, DHCP, and the settings file, use the `FILE_SERVER_URL` parameter to assign the file server address.

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

- HTTPSRVR, HTTPDIR and HTTPPORT parameters for an HTTP server.
- TLSSRV, TLSDIR and TLSPOST parameters for an HTTPS server.

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

Setting up a file server

About this task

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

Procedure

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

Avaya Vantage™ supports any HTTP or HTTPS server software as long as the software is correctly configured. Contact your server software vendor to obtain server software installation and configuration instructions.

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.

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™ Basic in networks controlled by Avaya SBCE, you must configure the Avaya Vantage™ Basic SIP user agent on Avaya SBCE.

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

- <Application Version> is the version of the Avaya Vantage™ Basic application. For example: 1.0.0.0
- <Build number> is the build number of the Avaya Vantage™ Basic application. For example: 0302
- ro.product.model is the MODEL4 value.

The following is an example of the configured Avaya Vantage™ Basic SIP user agent: Avaya Vantage Basic/1.0.0.0 0302;ro.product.number.

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

Avaya Aura® System Manager configuration

Configure the Avaya Aura® System Manager server to:

- Create users for telephony applications installed on Avaya Vantage™, such as Avaya Equinox™ and Avaya Vantage™ Basic.
- Manage public contacts and shared addresses.
- Use Personal Profile Management (PPM).

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, such as PROCPSWD.
- 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.

CSDK-based applications, such as Avaya Vantage™ Basic, 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.

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. If the PPM server is unreachable, Avaya Vantage™ tries the next IP address from SIP_CONTROLLER_LIST.

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.

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

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

Device configuration

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

- DHCP
 - Standard
 - Option 43
 - Option 242
- `46xxsettings.txt` file
- Avaya Aura® Device Services
- LLDP
- PPM
- Settings menu on the device

 Note:

The order might be different for some parameters. For more information, see the required parameter description in the “Supported configuration parameters” appendix.

 Note:

For more information about configuring Avaya Vantage™ using Avaya Aura® Device Services and PPM, see *Administering Avaya Aura® Device Services*.

Most of the 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 values provided by this source for the parameter.

Avaya Vantage™ modes

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 the Avaya Breeze™ CSDK-based application, Avaya Vantage™ operates in Avaya Breeze™ CSDK application based mode. When in this mode, Avaya Vantage™ supports the Login screen and configuration sharing.
- If the ACTIVE_CSDK_BASED_PHONE_APP is set to the default value (""), Avaya Vantage™ operates in the non Avaya Breeze™ CSDK application based 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 telephony applications will not use the configured values. For more information about whether a parameter is supported in the non Avaya Breeze™ CSDK application based mode, see the required parameter description in the "Supported configuration parameters" appendix.

When in non Avaya Breeze™ CSDK application based mode, backing up of the user configuration on PPM is not supported. If a parameter supports backing up on PPM and is supported in non Avaya Breeze™ CSDK application based mode, then this parameter will keep the configured value unless the user reverts to the factory default settings of the device.

Important:

The ACTIVE_CSDK_BASED_PHONE_APP must only be used when the active phone application is an Avaya Breeze™ CSDK application, such as Avaya Equinox™ or Avaya Vantage™ Basic. Otherwise, this parameter must use the default value.

Device configuration using DHCP options

Avaya Vantage™ connects to the DHCP server during the boot up. 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

Configurable DHCP options

The following options can be configured on the DHCP server:

Option	Description
Option 43	Specifies the encapsulated vendor-specific options that clients and servers use to exchange information. To use this option, Avaya Vantage™ sends option 60 with the value ccp.avaya.com. 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

Table continues...

Option	Description
	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 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 default value is 1000.
Option 60	Specifies the vendor class identifier. To use option 43, Avaya Vantage™ sends 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 • TLSSVR

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 codes supported by option 43 and the corresponding parameters are listed in the following table:

Code	Parameter
1	Does not set any parameter. The value must be 6889.
2	HTTPSRVR
3	HTTPDIR
4	HTTPPORT
5	TLSSVR

Table continues...

Code	Parameter
6	TLSDIR
7	TLSPORT
8	TLSSRVRID
9	L2Q
10	L2QVLAN
15	SIP_CONTROLLER_LIST
18	FILE_SERVER_URL

Avaya Vantage™ uses information from option 43 only if the first code of option 43 is 1 with a value of 6889. All values are interpreted as strings of ASCII characters. Avaya Vantage™ ignores invalid values and does not set the corresponding parameters.

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.
DNSSRV	The value of Option 6, if received, which might be a list of IP addresses.
HTTPSRVR	• The siaddr value, if 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 may be a list of IP addresses or DNS names.
SNTPSRV	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 Virtual Local Access Network that the device must connect to,
- The ICMPDU parameter defines that Destination Unreachable messages must not be transmitted.

```
HTTPSRVR="135.51.77.120,135.51.77.139",L2QVLAN=5,ICMPDU=0
```

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

To use configuration parameters on Avaya Vantage™, you must specify the option in the **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 URL for downloading image and configuration files. This parameter has higher precedence over HTTPSRVR, HTTPPORT, HTTPDIR, TLSSVR, TLSDIR, and TLSPOST.
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 data 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 <code>SET HTTPDIR=<path></code> . In configurations where the upgrade and binary files are in the default directory on the HTTP server, do not use the <code>HTTPDIR=<path></code> .
HTTPPORT	Destination port for HTTP requests. The default value is 80.
HTTPSRVR	IP addresses or DNS names of HTTP file servers used for downloading settings and firmware files during startup.

Table continues...

Parameter	Description
	Because the firmware files are digitally signed, TLS is not required for security. But 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.
PROCPSWD	Security string used to access local procedures. The default value is 27238.
REUSETIME	Specifies IP address reuse timeout, in seconds. The default value is 60.
SIP_CONTR OLLER_LIST	SIP proxy or registrar server IP or DNS addresses that can be 0 to 255 characters. Enter the IP address in the dot-decimal notation. For example: 127.0.0.1. You can provide several IP addresses separated by commas and without spaces between entries. The default is null, which means there are no controllers.
TIMEZONE	Time zone configuration in the Olson name format. For example, <i>America/New_York</i> or <i>Europe/Isle_of_Man</i> .
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.
TLSSVR	IP addresses or DNS names of Avaya 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_SERV ER_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 DHCP OFFER 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.

Configuring 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.
4. Save the `46xxsettings.txt` file.

Result

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

Customizing 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.

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

Item	Description	Structure	Example
Tag	Specifies a string in the file. Avaya Vantage™ navigates to that string when it interprets the corresponding <code>Goto</code> 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 <code>Goto</code> 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	<pre>IF \$<PARAMETER_NAME> SEQ <REFERENCE_VALUE> GOTO <TAG_NAME></pre>	<pre>IF \$MODEL4 SEQ K175 GOTO K175SETTINGS</pre>
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.	<pre>SET <PARAMETER_NAME> <PARAMETER_VALUE></pre>	<pre>SET FILE_SERVER_URL http://192.168.125.161</pre>
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.	<pre>GET <FILE_NAME></pre>	<pre>GET Settings.txt</pre>
Comment	Provides additional information about the	A string started with two pound characters (##).	<pre>## The following section contains</pre>

Table continues...

Item	Description	Structure	Example
	configuration process. Avaya Vantage™ does not interpret comments.	## <COMMENT>	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 ("").

Configuring user groups in the settings file

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

The following example shows simple settings file configuration for two user groups with 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 ##
GOTO END
# MANAGERS
## Section with parameters for Group 35 ##
# END
```

After configuring user groups in the settings file, you need to assign a specific user group to a device. For more information, see [Setting a user group for a specific configuration](#) on page 46.

Device configuration using LLDP

LLDP overview

Link Layer Discovery Protocol (LLDP) is an open standards layer 2 protocol that IP deskphones use to advertise their identity and capabilities and to receive administration from an LLDP server. LAN equipment can use LLDP to manage power, administer VLANs, and provide some administration. The transmission and reception of LLDP is specified in [IEEE 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.

- 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.

Avaya Vantage™ does not transmit LLDP frames over Ethernet if Wi-Fi is selected as a network mode.

After receiving of 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.
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

Table continues...

LLDP field	Value
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	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. 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	TIA LLDP MED Network Policy (Voice Signaling)	VLAN_IN_USE - set to the VLAN ID in the TLV. This TLV is ignored if: • The value of USE_DHCP is 0 and the value of IPADD is not 0.0.0.0. • The Application Type is not 1 (Voice) or 2 (Voice Signaling). • The Unknown Policy Flag (U) is set to 1.
SIP_CONTROLLER_LIST	Proprietary Call Server TLV	SIP_CONTROLLER_LIST will be set to the IP addresses 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.
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 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.	

Table continues...

No.	Task	Notes	✓
2.	Ensure that you are using Administrator mode.	Improper modification of some settings can lead to a device malfunction. Such settings are available to administrators only.	
3.	Configure file server data.	You must provide an address of a file server used to store software distribution packages and settings files.	
4.	Configure 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. If DHCP is not used, you must configure DNS server data statically.	
5.	Configure a user group.	You must specify a user group number to provide configuration parameters according to the assigned user group.	
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.	
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. Configure SIP settings through the Settings menu of the device if the <code>46xxsettings.txt</code> file cannot be downloaded.	
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.	
9.	Configure access to third party applications.	Specify which applications users can install.	

Administrator password configuration

You must set up an administrator password to enable administrator settings on Avaya Vantage™. Avaya Vantage™ uses the ADMIN_PASSWORD and PROCPSWD parameters to store the password and provide access to administrator settings.

- 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. The default value of PROCPSWD is 27238.
- If ADMIN_PASSWORD is not configured and PROCPSWD uses the default value, you cannot access administrator settings.

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

- `name=value` pair in a DHCPACK message sent by your DHCP server.
- PPM service configuration. For more information about setting the administrator password on PPM, see *Administering Avaya Aura® Session Manager*.

Enabling administrator settings on the device

About this task

You can enable administrator settings on Avaya Vantage™. In Administrator mode, the device displays menu items that are not available to end users, such as the **SIP proxy settings** menu.

Procedure

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

Setting up a file server address

About this task

Use this procedure to set up a file server address for downloading software distribution packages and settings files. 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™.

Procedure

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

A file server URL must have the following format:

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

In the URL:

- `hostname` is either an IP address in dotted-decimal format or a domain name.
- `port` is an optional port number.
- `path` is an optional path to a directory where distribution packages and other files are stored.

Setting the DNS name and address

About this task

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

Procedure

1. From the Home screen, tap **Applications**.
2. Tap **Settings**.
3. Tap **More > DNS**.
4. Tap **DNS Server**.
5. Enter the IP address of the primary DNS server in **DNS Server 1**.
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

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

Procedure

1. From the Home screen, tap **Applications**.
2. Tap **Settings**.
3. Tap **More > Avaya Aura Device Services (AADS)**.
4. Enter the address of the Avaya Aura® Device Services server and tap **OK**.

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. From the Home screen, tap **Applications**.

2. Tap **Settings**.
3. Tap **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 the server names to bypass the proxy server.

Procedure

1. From the Home screen, tap **Applications**.
2. Tap **Settings**.
3. Tap **More > HTTP/S Proxy Settings**.
4. Tap **Proxy host name[:port]**.
5. Enter the HTTP proxy host name with a port number.
6. Tap **OK**.
7. Tap **Bypass proxy for**.
8. Enter one or more server names to bypass the proxy server. Use the comma sign to separate server names.
9. Tap **OK**.

Configuring SIP server settings

About this task

Use this procedure to register Avaya Vantage™ to the SIP server.

Procedure

1. From the Home screen, tap **Applications**.
2. Tap **Settings**.
3. Tap **More > SIP Settings**.
4. Tap **SIP domain**.
5. Enter the server name for registration.
6. Add a SIP server to the SIP servers list:
 - a. Tap **SIP proxy settings**.
 - b. In the upper right corner, tap **Add**.

- c. Enter the name of the SIP proxy server in the **SIP proxy server** field.
You can use either the dotted-decimal or DNS name format.
- d. From the **Transport type** field, select the TLS or TCP protocol for the SIP server.
Avaya Vantage™ does not support UDP.
- e. **(Optional)** Enter a port number that will be used by the server in the **SIP port** field.
Avaya Vantage™ uses the following default port numbers:
 - 5060 for TCP
 - 5061 for TLS

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. You can only set the SSON using the **Settings** menu of Avaya Vantage™.

Procedure

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

The number must be in a range between 124 and 254.

Security configuration

Avaya Vantage™ provides lock and logout functionality for the protection of user privacy. Each user has their own login and password, so when a user locks Avaya Vantage™, other users cannot unlock the device. When Avaya Vantage™ is in a locked state, you can receive calls or make emergency calls. Avaya Vantage™ restricts access to any user data while in the locked state. As an administrator, you can enable or disable the locked state using the ENABLE_PHONE_LOCK Settings file parameter as described in [Phone lock parameters](#) on page 120. The locked state can also be manually set using **Screen lock** in the **Settings > Security** menu.

When a user logs out from Avaya Vantage™, the station is available for other users. However, when another user logs in to the same station, that user cannot access previous user's data. When a new user logs in, Avaya Vantage™ clears the previous user's personal data. When the user logs in again, Avaya Vantage™ restores the following information:

- User-defined device configuration, such as language settings.
- Application data that is backed up using a personal account, such as a Google™ account.

For troubleshooting, Avaya Vantage™ supports the Secure Shell Protocol (SSH) and a secure mechanism for personnel to log in to the device remotely and perform the required operations in a secure environment. By default, SSH 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.

To enable SSH, Avaya Vantage™ uses the SSH_ALLOWED parameter.

Avaya Vantage™ does not support insecure services, such as FTP, Telnet, TFTP, rlogin, rsh, and so on. The only exception is support of Android Debug Bridge (ADB). By default, ADB is disabled and can be enabled using the **Settings** menu on the device. You can completely disable ADB support using the ADBSTAT parameter.

To enhance security, Avaya Vantage™ supports the Secure Real-time Transport Protocol (SRTP), which provides confidentiality and message authentication to media traffic going over the LAN infrastructure. This allows the Avaya Vantage™ to encrypt calls between two or more endpoints, to prevent anyone from eavesdropping.

Some of the other security features are:

- TLS support for all services, such as PPM, HTTP file downloads, Avaya Aura® Device Services connection, and SCEP over HTTPS.
- 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-TTLS, and EAP-PWD with phase two authentication.
- Identity certificate and trusted certificate support. Avaya Vantage™ supports up to 100 trusted certificates in either PEM or DER format.
- Android built-in certificates which can be used by all Android applications installed on Avaya Vantage™.
- No built-in Avaya certificates except Avaya Product Root CA. This certificate is only used for software signature validation.
- Application download control using a configurable XML file. No installation of applications from unknown sources.
- Support for antivirus and antimalware applications.
- Android security features, such as disk encryption, remote wipe, and SELinux running in enforcing mode.

Password security policies

In SIP login password you can use:

- Numerics: 0 – 9
- Uppercase letters: A – Z
- Lowercase letters: a – z
- Special characters: ~!@#%&* _+=`|()\{}[]:;'"<>,.?/

You can configure password policies for Avaya Vantage™ using System Manager.

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, the user might not be able to configure or use the 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 Microsoft Exchange Server security policies. Avaya Vantage™ uses the Unified Login credentials to access the Exchange account.

Certificate management

Digital certificates are electronic documents used to confirm the identity of the device or application. A number of Avaya Vantage™ applications use these certificates:

- Avaya Vantage™ platform applications:
 - Android: Wi-Fi 802.1x authentication, Exchange and Google accounts, and browsers using HTTPS.
 - Avaya: Configuration and firmware file downloads using HTTPS, SCEP over HTTPS, Avaya Aura® Device Services or Authenticated file server, and PPM.
- Communication applications: Use certificates for different activities, such as SIP connectivity using SIP over TLS and PPM over TLS and connection to Avaya Aura® Device Services servers.

Avaya Vantage™ downloads trusted digital certificates and a PKCS12 file, and generates the identity certificate using SCEP.

The downloaded trusted certificates are stored in the Android trust store under the “VPN and APPS” and “Wi-Fi” repositories. These certificates are available for all applications, including third party applications. The “Wi-Fi” repository contains only the downloaded trusted certificates. The “VPN and APPS” repository contains the Android built-in CA certificates and the downloaded trusted certificates.

To store built-in Android certificates and downloaded certificates, Avaya Vantage™ uses the Android certificate store.

By default, users can install and review installed trusted and identity certificates. To restrict certificate installation, system administrators can provide a list of applications that can install certificates using the CERT_INSTALL_APPLICATION_LIST parameter. If this parameter is configured to "", then only the Avaya Vantage™ platform can change or update trusted certificates using the TRUSTCERTS configuration parameter. Avaya Vantage™ downloads trusted certificates and adds these certificates to the Android certificate store.

*** Note:**

For security reasons, it is recommended to use the "" value for CERT_INSTALL_APPLICATION_LIST.

Avaya Vantage™ downloads a PKCS12 file from a URL specified in the PKCS12URL configuration parameter. If the PKCS12PASSWORD configuration parameter does not contain the valid password for the PKCS12 file, Avaya Vantage™ prompts users to enter the password using UI. If the PKCS12 file contains a trusted certificate, Avaya Vantage™ will not download this certificate.

Identity certificates are stored in the system credential storage under the "VPN and APPS" and "Wi-Fi" repositories. Only Avaya Vantage™ platform applications and Avaya applications, such as Avaya Vantage™ Basic, can access the system credential storage. Third party applications can access identity certificates only if these applications are specified in the ID_CERT_APPLICATION_LIST configuration parameter.

You can review certificates installed on Avaya Vantage™ device:

- The **Settings > Security > EASG trusted credentials** menu on the device contains EAGS certificates.
- The **Settings > Security > Trusted credentials** menu on the device contains CA certificates.
- The **Settings > Security > Client credentials** menu on the device contains identity certificates.

Certificate usage by applications

The following table shows certificates that are used by different applications on Avaya Vantage™:

Application	Built in Android trusted certificates	Downloaded trusted certificates	Identity certificate generated using SCEP or PKCS12 file
Wi-Fi 802.1x with EAP-TLS, EAP-TTLS	N	Y	Y
Ethernet 802.1x with EAP-TLS	N	Y	Y
HTTPS configuration and image files download	N	Y	Y
PPM	N	Y	Y

Table continues...

Application	Built in Android trusted certificates	Downloaded trusted certificates	Identity certificate generated using SCEP or PKCS12 file
SCEP over HTTPS	N	Y	Y
Avaya Aura® Device Services or Authentication file server	N	Y	Y
Browser	Y	Y	N
Exchange account	Y	Y	Y
Google account	Y	Y	N
Approved third party applications (included in ID_CERT_APPLICATION_LIST)	Y	Y	Y
Non-approved third party applications (not included in ID_CERT_APPLICATION_LIST)	Y	N	N

Configuring security parameters

For secure installation, configure the following parameters.

Parameter	Set to	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 one hundred certificate files. Avaya Vantage™ supports both PEM and DER file formats.
TLSSRVRID	1	Certificates installed on servers must have the common name that matches the device configuration.
AUTH	1	Ensures usage of HTTPS file servers for configuration and software files 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.
SSH_ALLOWED	0	Keeps Secure Shell (SSH) disabled.
ADBSTAT	0	Keeps Android Debug Bridge (ADB) disabled.

SCEP parameters

Configure the following Simple Certificate Enrollment Protocol (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 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 media access control (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 a certificate enrollment. The range is from 1024 to 2048.
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. 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.
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.
PKCS12URL	String	Null	Specifies the URL where a PKCS12 file containing an identity certificate is stored.
PKCS12PASSWORD	String	Null	Specifies a PKCS12 password.
ID_CERT_APPLICATION_LIST	String	all	Specifies applications that can install trusted and identity certificates stored on Avaya Vantage™.
ID_CERT_APPLICATION_LIST	String	all	Specifies applications that can access trusted and identity certificates stored on Avaya Vantage™.

Table continues...

Parameter	Type	Default value	Description
SCEPPASSWORD	String	\$SERIALNO	Specifies a challenge password to use with SCEP. The value of SCEPPASSWORD, if non-null, is included in a challengePassword attribute in SCEP certificate signing requests. If the value contains \$SERIALNO, \$SERIALNO is replaced by the value of SERIALNO. If the value contains \$MACADDR, \$MACADDR is replaced by the value of MACADDR without the colon separators.

VLAN

Configure the following Virtual local area network (VLAN) parameters:

Parameter	Set to	Notes
L2Q	0, 1, or 2	Specifies 802.1Q VLAN tagging mode. Assign one of the following values: - Auto (0): The device sends tagged packets on L2QVLAN. If the DHCP server is unreachable, the device sends untagged packets until the VLANTEST time. - Tag (1): The device sends tagged packets on L2QVLAN. If the DHCP server is unreachable, the device sends tagged packets with VLAN equals to 0 until the VLANTEST time. - Untag (2): The device sends untagged packets.
L2QVLAN	Non-zero value	The 802.1Q VLAN identifier.

For the above VLAN configuration, the full VLAN separation between the device and computer packets is used. The device tries to obtain an IP address from the DHCP server on the voice VLAN. If the device gets an IP address, the device sends all the tagged packets on the voice LAN. Tagged packets from VLAN computers other than the data VLAN are blocked.

Chapter 5: Application setup

Avaya Vantage™ supports the installation of applications. Applications can be installed using:

- The “Push application” method. To push an application on the device, the administrator provides the path to the application package 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. End users can download applications from Google Play. The system administrator can restrict installation of certain applications using a configuration file.

Pushing applications onto the Avaya Vantage™ device

About this task

Use this procedure to push applications to Avaya Vantage™.

Before you begin

Ensure that you have the application package file and the `46xxsettings.txt` settings file.

Procedure

1. Open the `46xxsettings.txt` settings file in a text editor.
2. If the settings file contains the string `SET PUSH_APPLICATION <a list of URLs>`, do the following:
 - a. If the list of URLs contains a URL where the previous version of the application package file is located, delete this URL from the list.
 - b. If the list of URLs contains at least one entry, enter a comma after the last entry.
 - c. Enter the URL where the application package file is located.

 Note:

If the application package file is stored in the root directory of your HTTP or HTTPS server, you can provide the file name only. If the application package file is stored in a

subdirectory of your HTTP or HTTPS 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. If the settings file does *not* contain the string `SET PUSH_APPLICATION <a list of URLs>`, do the following:
 - a. Add a new string with the text `SET PUSH_APPLICATION` followed by a space.
 - b. Enter the URL where the application package file is located.
4. Save the settings file.
5. Upload the settings file on the file server.

Result

On the next polling period, Avaya Vantage™ downloads the settings file and pushes the application on the device.

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_1.0.0.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_1.0.0.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.

Administering access to Google Play applications

Google Play is the main source of Android applications. According to your company's policies you can determine:

- Whether end users can install applications on Google Play.
- Which applications end users can install on Google Play.

Access to Google Play is set up using the `USER_INSTALL_APPS_GOOGLE_PLAY_STORE` parameter in the `46xxsettings.txt` file.

The availability of certain applications is determined by completing black and white list sections in an XML-based configuration file:

- Black list: End users cannot install applications from the black list. If the black list is empty, users can install any third-party application on Google Play.
- 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 is empty, users cannot install applications on Google Play.

If the configuration file is not specified, users can install any application on Google Play.

The `APPS_CONTROL_FILE` parameter defines the location of the configuration file.

Editing black and white lists

Before you begin

Create a third party applications configuration file if you do not have one.

Procedure

1. Open the `46xxsettings.txt` settings file in a text editor.
2. To edit the black list, in the `<allowedUserInstalledAppsUsingGooglePlayStore type="blacklist">` section, list the applications you want to include.

Use the following format: `<app package name="<Type the package name here>" />`.

```
<allowedUserInstallAppsUsingGooglePlayStore type="blacklist">
  <app package name="com.restricted.application" />
  <app package name="com.hacker.software" />
</allowedUserInstallAppsUsingGooglePlayStore>
```

3. To edit the white list, in the `<allowedUserInstalledAppsUsingGooglePlayStore>` section, list the applications you want to include.

Use the following format: `<app package name="<Type the package name here>" />`.

```
<allowedUserInstallAppsUsingGooglePlayStore>
  <app package name="com.avaya.communicator" />
```

```
<app package="com.elansimpleapp" />
</allowedUserInstallAppsUsingGooglePlayStore>
```

4. Save the settings file.
5. Upload the file on the file server.

Result

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

Setting up a CSDK-based telephony application as the active application

About this task

If you want to use a CSDK-based telephony application as the active telephony application, you need to set up the ACTIVE_CSDK_BASED_PHONE_APP parameter. If the parameter is not set, the application might not function properly. For more information about parameter values, see [Package names of CSDK-based applications](#) on page 59.

! Important:

Only one CSDK-based application can be the active telephony application at a time, so ACTIVE_CSDK_BASED_PHONE_APP must contain only one package name.

Before you begin

Install the telephony application on Avaya Vantage™.

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 SET ACTIVE_CSDK_BASED_PHONE_APP "a name of the application package".
4. Save the settings file.
5. Upload the settings file on the file server.

On the next polling period, Avaya Vantage™ downloads the settings file and updates the parameter value.

6. When prompted, reboot Avaya Vantage™.

Avaya telephony applications supported on Avaya Vantage™

In the current release, Avaya Vantage™ supports the following Avaya telephony applications:

Application	Avaya Breeze™ CSDK-based?
Avaya Vantage™ Basic	Yes
Avaya Equinox™	Yes
Avaya Vantage™ Open	No

If you want to use an CSDK-based telephony application, you also need to set up the ACTIVE_CSDK_BASED_PHONE_APP parameter. For more information, see [Package names of CSDK-based applications](#) on page 59.

Package names of CSDK-based applications

The following table shows package names of the CSDK-based phone applications. If you want to use the CSDK-based phone application, you need to set the ACTIVE_CSDK_BASED_PHONE_APP parameter using the corresponding package name.

Application	Package name
Avaya Equinox™	"com.avaya.android.flare"
Avaya Vantage™ Basic	"com.avaya.android.vantage.basic"

Chapter 6: Maintenance

Device upgrade

You should upgrade Avaya Vantage™ software to keep the device up-to-date, to gain access to new features, and to enhance stability and security.

Avaya Vantage™ downloads upgrade images and configuration files from a file server using HTTP or HTTPS.

Before upgrading the device, perform the following actions:

- Download the newest distribution package and `46xxsettings.txt` settings file on the file server.
- Provide a path to the file server in the `FILE_SERVER_URL` configuration parameter.

 Note:

If `FILE_SERVER_URL` is not defined, Avaya Vantage™ will use `HTTPSRRV`, `HTTPPORT`, and `HTTPDIR` for a HTTP file server or `TLSSRRV`, `TLSPORT`, and `TLSSIR` for a HTTPS file server.

You can perform the device upgrade in the following ways:

- Automatic: You can configure the device to poll periodically for a newer version of the software in the file server and automatically download the upgraded software.
- Manual: You can upgrade the device manually without the device waiting for a polling interval by:
 - Using the **Update** option in the **Settings** menu of 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** menu of the device or from System Manager. If an updated version of firmware is available, then the device upgrades immediately after reboot or later according to the upgrade policy configured for the device.

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. The upgrade image stores information about packages in a `Package.gz` file. This file contains a list of all packages in the image and provides information about versions for each package. Using

packages can reduce download times, network traffic, and the resets required to complete the upgrade.

Avaya Vantage™ does the following to perform an upgrade:

1. Avaya Vantage™ receives the file server address from DHCP, LLDP, or the device interface.
2. Avaya Vantage™ connects to the file server and searches for the `K1xxSupgrade.txt` file.
3. Avaya Vantage™ compares its software version with the version specified in the `K1xxSupgrade.txt` file.
4. If a newer version of the software distribution package is available, Avaya Vantage™ downloads `Packages.gz` and determines which packages can be upgraded.
5. Avaya Vantage™ downloads and installs the required packages if no error occurs.
6. Avaya Vantage™ also looks for the `46xxsettings.txt` settings file that is specified in the `K1xxSupgrade.txt` file and downloads this settings file.

Automatic upgrade

You can configure the settings file to allow Avaya Vantage™ to periodically check for a newer version of the 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.

You can specify the following upgrade policies in the settings file:

- Schedule download for a specific time and day in a week
- Schedule installation on a specific date and time
- Set the polling interval for a new image file

Automatic upgrades do not interrupt active calls. Avaya Vantage™ starts the upgrade after the user completes all calls.

Upgrading Avaya Vantage™ using System Manager

About this task

Use this procedure to perform a bulk upgrade of Avaya Vantage™.

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.

The actual procedure might differ depending on the System Manager version you use. For more information about the procedure, refer to *Administering Avaya Aura® System Manager*.

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 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 screen.
2. Tap **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.

Restoring factory settings

About this task

Use this procedure to remove all user information stored on the device and to restore original manufacturer settings.

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

- All administered values.
- User-specified data, including information about all accounts.
- Device settings.
- Application data and settings.
- Wi-Fi network configuration.

You cannot recover settings and data after you delete them.

Procedure

1. From the Home screen, tap **Applications**.
2. Tap **Settings**.

3. Tap **Menu > Admin login** in the upper-right corner of the screen and enter the administrator password.
4. Tap **Backup & reset > Factory data reset**.
5. Tap **Reset device**.
6. Tap **Erase everything**.

Rebooting Avaya Vantage™

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 screen.
2. Tap **Backup & reset**.
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 the device

Enabling verbose logging

About this task

Use this procedure to set the scope of log messages and the events that must be included in log messages.

Procedure

1. From the Home screen, tap **Applications**.
2. Tap **Settings**.
3. Tap **Debugging options**.
4. **(Optional)** If the **Log** option is not available on the Debugging and monitoring options screen, tap **Admin login** and enter the administrator password.
5. Tap **Log**.
6. Tap **Log Categories** and select the log categories to be included in log messages.
7. Tap **Remote Logging** to configure parameters for system logging.
 - a. Select the **Remote Logging** check box to enable system logging.
 - b. From the **Remote Log Level** list, select the events to be included in log messages.
By default, logs only include errors.
 - c. In the **Remote log server** field, provide the address of the server where you want logs to be stored.
8. Tap **Local logging** to configure parameters for local logging.
 - a. Select the **Local Logging** check box to enable local logging.
 - b. From the **Local Log Level** list, select the events to be included in log messages.
By default, logs only include errors.
 - c. Tap **Clear Local Log Files** to delete local logging files and core dump files.

Generating a debug report

About this task

Use this procedure to generate a debug report. You can save the report in the internal flash memory of Avaya Vantage™ or on an HTTP or HTTPS server. Ensure that the debug password is recorded properly because the report is encrypted and cannot be decrypted without the password.

Procedure

1. From the Home screen, tap **Applications**.
2. Tap **Settings**.
3. Tap **Debugging options > Debug report > Generate debug report**.
4. Enter the password and select the destination location.
5. Tap **Generate**.

Result

Avaya Vantage™ generates a debug report and stores it in the `/var/log/Brio_debug_report/debugreport.tar.gz` file.

Opening a debug report

About this task

Avaya Vantage™ encrypts a debug report. To review debug data, you must decrypt the report.

Procedure

1. To decrypt the report, run the following command:

```
openssl aes-128-cbc -d -salt -k <password> -in debugreport.tag.gz -out  
debugreport.decrypted.tag.gz
```

In this command, <password> is the password that you provided when generating the report.

Avaya Vantage™ stores the decrypted report in the `debugreport.decrypted.tag.gz` archive file.

2. To extract the 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 debugreport.decrypted.tag.gz
```

.

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.

Procedure

1. From the Home screen, tap **Applications**.
2. Tap **Settings**.
3. Tap **Debugging options** > **Host to ping**.
4. Enter the IP address or host name of the device.
5. Tap **OK**.

Avaya Vantage™ displays ping messages if the station can resolve the IP address.

Chapter 7: 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.

Solution

Use the boot recovery procedure to clear the device and restore Avaya Vantage™ to its factory settings.

1. Reboot the device.
2. 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**.

3. Tap **Enter BRM** to navigate to Avaya Vantage™ boot recovery options.
4. Enter the administrator password.

Avaya Vantage™ starts the boot recovery procedure and displays a list of options.

5. 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.

Chapter 8: Resources

Documentation

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

Title	Use this document to:	Audience
Overview		
<i>Avaya Aura® Session Manager Overview and Specification</i>	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
Implementing		
<i>Deploying Avaya Aura® Session Manager</i>	Deploy Avaya Aura® Session Manager.	Implementation personnel and service administrators
<i>Upgrading Avaya Aura® Session Manager</i>	Upgrade Avaya Aura® Session Manager.	Implementation personnel and service administrators
<i>Deploying Avaya Aura® System Manager on System Platform</i>	Deploy Avaya Aura® System Manager.	Implementation personnel and service administrators
<i>Deploying Avaya Aura® Conferencing: Basic Installation</i>	Deploy Avaya Aura® Conferencing.	Implementation personnel and service administrators
Administering		
<i>Administering Avaya Aura® Session Manager</i>	Administer and maintain Avaya Aura® Session Manager.	System administrators
<i>Administering Avaya Aura® System Manager</i>	Administer and maintain Avaya Aura® System Manager.	System administrators
<i>Administering Avaya Aura® Conferencing</i>	Administer Avaya Aura® Conferencing.	System administrators
<i>Administering Avaya Session Border Controller for Enterprise</i>	Administer Avaya Session Border Controller for Enterprise.	System administrators

Table continues...

Title	Use this document to:	Audience
<i>Administering Avaya Vantage™ Open</i>	Administer the Media and Provisioning Server required to perform calls using Avaya Vantage™ Open.	System administrators
Maintaining		
<i>Maintaining Avaya Aura® Session Manager</i>	Maintain Avaya Aura® Session Manager.	System administrators and IT personnel
<i>Troubleshooting Avaya Aura® Session Manager</i>	Troubleshoot known issues for Avaya Aura® Session Manager.	System administrators and IT personnel
Using		
<i>Using Avaya Vantage™ Basic</i>	Use Avaya Vantage™ Basic.	• End users • Support personnel
<i>Using Avaya Equinox™ for Android, iOS, Mac, and Windows</i>	Use Avaya Equinox™.	• End users • Support personnel
<i>Using Avaya Vantage™ Open</i>	Use Avaya Vantage™ Open.	• End users • Support personnel

Finding documents on the Avaya Support website

Procedure

1. Navigate to <http://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 an appropriate release number.

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 displays the documents only from the selected category.

7. Click **Enter**.

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.

Procedure

- To find videos on the Avaya Support website, go to <http://support.avaya.com> and perform one of the following actions:
 - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
 - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
 - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

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

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 <code>46xxsettings.txt</code> settings file. For provisioning, use the Settings > Wireless & networks > More > Group menu on the device. This parameter is supported in all modes.
AUTH	Numeric	0	No	Authentication flag for all file downloads, including configuration files 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 <code>SET</code> command in the <code>46xxsettings.txt</code> file. This parameter is supported in all modes.

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 telephone's apparatus code. The length is from 8 to 10 ASCII characters. This parameter can be used in conditional statements in the <code>46xxsettings.txt</code> file. This parameter cannot be modified. This parameter is supported in all modes.
MODEL4	String	Factory settings	No	Name of the telephone model or the truncated model identifier. This parameter can have one of the following values: • K175 for Avaya Vantage™ with a camera. • K165 for Avaya Vantage™ without a camera. This parameter can be used in conditional statements in the <code>46xxsettings.txt</code> file. This parameter cannot be modified. This parameter is supported in all modes.
MACADDR	String	Factory settings	No	Media Access Control (MAC) address of the telephone. MACADDR contains six pairs of ASCII hexadecimal characters separated by colons. This parameter can be used in conditional statements in the <code>46xxsettings.txt</code> file. This parameter is supported in all modes.

General phone functionality

Parameter	Type	Default value	Is set to default on reset	Description
BRANDING_VOLUME	Numeric	5	Yes	Specifies the level of the Avaya audio brand. Assign one of the following values: • 8: 9 db above nominal

Parameter	Type	Default value	Is set to default on reset	Description
				• 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 This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

Phone UI related settings

Common operations

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.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> file. - The Settings > Audio settings > Headset signalling menu on the device. This parameter is supported in all modes. This parameter can be stored on the PPM or backup server.
BAKLIGHTOFF	Numeric	120	Yes	Timer to disable the backlight on the phone display. The range is from 0 to 999 minutes. This parameter is supported in all modes. For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> file. - The Settings menu on the device. This parameter can be stored on the PPM or backup server.
CLICKS	Numeric	1	No	Specifies whether touch sounds are enabled. 0: Touch sounds are disabled. 1: Touch sounds are enabled. This parameter is supported in all modes. For provisioning, use the Settings > Sound & notification > Other sounds > Touch sounds menu on the device. This parameter can be stored on the PPM or backup server.
LARGEFONT	Numeric	1	Yes	Specifies the size of the font. Assign one of the following values: 3: Huge font size. 2: Large font size. 1: Normal font size. 0: Small font size. This parameter is supported in all modes.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				For provisioning, use the Settings > Display > Font size menu on the device. This parameter can be stored on the PPM or backup server.
INITIAL_SCREEN	String	ADMIN	Yes	Specifies the initial screen presented to a user after logging in to Avaya Vantage™. Assign one of the following values: • PHONE • HOMESCREEN • ADMIN For provisioning, use the Settings > Display > Screen presented after login menu on the device. This parameter is <i>not</i> supported in the non Avaya Breeze™ CSDK application based mode. This parameter can be stored on the PPM or backup server.
ADMIN_INITIAL_SCREEN	String	HOME	Yes	This parameter specifies whether the Home screen or Telephony screen is presented as the initial screen after the user logs in to Avaya Vantage™. Assign one of the following values: • PHONE • HOMESCREEN This parameter is <i>not</i> supported in the non Avaya Breeze™ CSDK application based mode. For provisioning, use the SET command in the 46xxsettings.txt file.

Specific audio settings

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. This parameter is supported in all modes.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> file. - The Settings > 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. This parameter is supported in all modes. For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> file. - The Settings > 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. This parameter is supported in all modes. For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> file. - The Settings > 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.
AUDIOSTHD	Numeric	0	Yes	Specifies headset sidetone settings. The options are: 0: Normal level.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				• 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 in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> 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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
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 <code>HEADSET_PROFILE</code> is 0, the headset audio profile is not selected. This parameter is supported in all modes.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				For provisioning, use the Settings > 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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> 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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file. For example, to rename the first and third profiles and to retain the default name of the second profile, enter the following: <code>SET HEADSET_PROFILE_NAMES "Profile 1,,Profile 3"</code>
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 <code>HANDSET_PROFILE</code> is 0, the handset audio profile is not selected. This parameter is supported in all modes. For provisioning, use the Settings > Audio settings > Handset profile menu on the device.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> 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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file. For example, to rename the first and third profiles and to retain the default name of the second profile, enter the following: <code>SET HANDSET_PROFILE_NAMES "Profile 1,,Profile 3"</code>

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 <code>LL[_CC]</code> format where: <code>LL</code> is a language code. The language code is represented by two lowercase letters. For example: <code>en</code>. For more information about codes, see ISO 639-1.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
USER_LANGUAGE_CHOICE	String	Null	No	Specifies the user language choice in the ISO format. The range is the default string length. This parameter is supported in all modes. For provisioning, use the Settings > Language & input > Language menu on the device.
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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> 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: <code>America/New_York</code>. For more information about the name format and for a list of time zones, see the Time Zone Database. This parameter is supported in all modes. For provisioning, use: DHCP option 242.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				The SET command in the <code>46xxsettings.txt</code> file.
USER_CHOICE_TIMEZONE	Integer	0	No	Specifies a time zone source for Avaya Vantage™. The options are: 0: Avaya Vantage™ uses the time zone specified in TIMEZONE. 1: Avaya Vantage™ uses the time zone specified in the Settings menu. This parameter is supported in all modes. For provisioning, use the Settings > Date & time > Select time zone menu on the device.
ADMINTIMEFORMAT	Integer	0	No	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 <code>46xxsettings.txt</code> file. This parameter is supported in all modes.

Network settings

The following sections describe network configuration settings, such as Ethernet, VLAN, QoS, and IEEE 802.1X.

General settings

Parameter	Type	Default value	Is set to default on reset	Description
IPADD	String	0.0.0.0	Yes	Specifies the IP address of the Avaya Vantage™ device. The range is from 7 to 15 ASCII characters. This is a testable parameter.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				The parameter can be used in conditional statements in the <code>46xxsettings.txt</code> file. This parameter is supported in all modes. For provisioning, use: • The <code>yiaddr</code> field value in the DHCPACK message. • For provisioning, use the Settings > Network > Ethernet > IP interface > Static IP settings menu on the device.
ROUTER	String	0.0.0.0	Yes	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. This parameter is supported in all modes. For provisioning, use: • The Option 3 value in a DHCPACK message. • For provisioning, use the Settings > Network > Ethernet > IP interface > Static IP settings menu on the device.
NETMASK	String	0.0.0.0	Yes	Specifies an IP subnet mask. This parameter specifies one IP address in the dot-decimal format. The range is from 7 to 15 ASCII characters. This parameter is supported in all modes. For provisioning, use: • The Option 1 value in a DHCPACK message. • For provisioning, use the Settings > Network > Ethernet > IP interface > Static IP settings menu on the device.
SUBNET	String	0.0.0.0	Yes	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. This parameter is supported in all modes. The parameter can be used in conditional statements in the <code>46xxsettings.txt</code> file.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
USE_DHCP	Numeric	1	Yes	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. This parameter is supported in all modes. For provisioning, use the Settings > Network > Ethernet > IP interface > Use DHCP menu on the device.
DHCP_SSON	Numeric	242	Yes	Specifies the site-specific option number for DHCP. The range is from 128 to 254. This parameter is supported in all modes. For provisioning, use the Settings > Wireless & networks > More > DHCP Site Specific Option Number (SSON) menu on the device.
DHCPSTD	Integer	0	Yes	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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
ICMPDU	Integer	1	Yes	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 in the range from 33,434 to 33,523. • 2: DU messages are transmitted.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				This parameter is supported in all modes. For provisioning, use: - A <code>name=value</code> pair in a DHCPACK message. - The SET command in the <code>46xxsettings.txt</code> file.
ICMPRED	Integer	0	Yes	Specifies whether Avaya Vantage™ proceeds ICMP redirect messages. Assign one of the following values: 0: Avaya Vantage™ does not proceed received redirect messages. 1: Avaya Vantage™ proceeds received redirect messages according to RFC 1122. This parameter is supported in all modes. For provisioning, use: - A <code>name=value</code> pair in a DHCPACK message. - The SET command in the <code>46xxsettings.txt</code> file.
MTU_SIZE	Integer	1500	Yes	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. This parameter is supported in all modes. For provisioning, use: - A <code>name=value</code> pair in a DHCPACK message. - The Option 26 value in the DHCPACK message. - The SET command in the <code>46xxsettings.txt</code> file.
REUSETIME	Integer	60	Yes	Specifies the IP address reuse timeout in seconds. The range is from 0 to 20,999. This parameter is only used for wired Ethernet connections.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				This parameter is <i>not</i> supported in the non Avaya Breeze™ CSDK application based mode. For provisioning, use: • The Option 242 value in the DHCPACK message. • The SET command in the <code>46xxsettings.txt</code> file.
NETWORK_MODE	Numeric	1	Yes	Specifies the active network interface. The available options are: • 1: Wired Ethernet connection is active. • 2: Wi-Fi connection is active. This parameter is supported in all modes. For provisioning, use the Settings > Network > Network mode menu on the device.
IPV6STAT	Numeric	1		Controls whether Avaya Vantage™ blocks all incoming and outgoing IPv6 traffic. • 0: Avaya Vantage™ blocks IPv6 traffic. • 1: Avaya Vantage™ does not block IPv6 traffic.  Important: You must set this parameter to 0 because Avaya Vantage™ does not support IPv6. This parameter is applicable for both wired Ethernet and wireless connections. This parameter is supported in all modes. For provisioning, use the SET command in the <code>46xxsettings.txt</code> file.
BLUETOOTHSTAT	Integer	1	Yes	Specifies whether Bluetooth is allowed for user configuration. Assign one of the following values: • 0: Bluetooth and the Bluetooth menu are disabled in Settings on the device. The user cannot enable Bluetooth. • 1: Bluetooth and the Bluetooth menu are enabled in Settings on the device. The user can enable or disable Bluetooth. This parameter is supported in all modes. For provisioning, use the SET command in the <code>46xxsettings.txt</code> file.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
BLUETOOTH_FEATURES_SHARED_VIA_STAT	Integer	0	Yes	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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
TRUST_AGENTS_STAT	Integer	1	Yes	Specifies whether users can configure trust agents. • 0: The Trust agents menu on the device is disabled. Users cannot access trust agents. All trust agents are disabled. • 1: The Trust agents menu on the device is enabled. Users can access trust agents. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
TRUST_AGENTS_SMARTLOCK_STAT	Integer	1	Yes	Specifies whether users can configure the Smart Lock Agent feature. • 0: Users cannot access Smart Lock in the Settings menu. Smart Lock Agent is disabled. • 1: Users can access Smart Lock in the Settings menu. Users can enable or disable the Smart Lock Agent feature. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
WIFISTAT	Integer	0	Yes	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 from Wi-Fi in the Settings menu. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
WIFIAPSTAT	Numeric	0	Yes	Specifies whether users can configure the WI-FI access point. • 0: WI-FI access point is disabled. User cannot enable the access point. • 1: Users can enable and configure the access point. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
WIFI_CON_STATU S_ON_LOGOUT	Numeric	1	Yes	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 <i>not</i> supported in the non Avaya Breeze™ CSDK application based mode. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
ADBSTAT	Numeric	1	Yes	Specifies whether Android Debug Bridge (ADB) is enabled. • 0: ADB is disabled and USB debugging is disabled in the Settings menu. • 1: ADB is disabled, but you can enable it from USB debugging in the Settings menu. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
GRATARP	Integer	0	Yes	Specifies whether an existing Address Resolution Protocol (ARP) cache entry is updated with a MAC 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.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

Ethernet interface settings

Parameter	Type	Default value	Is set to default on reset	Description
PHY1STAT	Numeric	1	Yes	Specifies the speed and duplex mode of Ethernet line interface. Assign one of the following values: • 1: Auto negotiation speed and duplex. • 2: 10Mbps half-duplex operation. • 3: 10Mbps full-duplex operation. • 4: 100Mbps half-duplex operation. • 5: 100Mbps full-duplex operation. This parameter is supported in all modes. For provisioning, use the Settings > Network > Ethernet > Interfaces > Ethernet 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 This parameter is supported in all modes. For provisioning, use: • A <code>name=value</code> pair in a DHCPACK message. The precedence is 1.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				• DHCP option 43. The precedence is 1. • The SET command in the <code>46xxsettings.txt</code> 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 > Ethernet > VLAN > VLAN tagging (802.1Q) menu on the device. The precedence is 5.
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. This parameter is supported in all modes. For provisioning, use: • A <code>name=value</code> pair in a DHCPACK message. The precedence is 1. • DHCP option 43. The precedence is 1. • The SET command in the <code>46xxsettings.txt</code> 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 > 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 DHCP OFFER message reception on a non-zero VLAN. The range is from 0 to 999.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				This parameter is supported in all modes. For provisioning, use: • A <code>name=value</code> pair in a DHCPACK message. • The SET command in the <code>46xxsettings.txt</code> file. • The Settings > Network > Ethernet > VLAN > VLAN test timer menu on the device.

IEEE 802.1X settings

Parameter	Type	Default value	Is set to default on reset	Description
DOT1XSTAT	Numeric	0	Yes	Specifies whether the IEEE 802.1X feature for Ethernet is enabled on Avaya Vantage™. The following options are available: • 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. This parameter is supported in all modes. For provisioning, use: • The SET command in the <code>46xxsettings.txt</code> file. • The Settings > Network > Ethernet > IEEE 802.1x authentication > Supplicant mode menu on the device.
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

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				The range is a default string length. This parameter is supported in all modes. For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> file. - The Settings > Network > Ethernet > IEEE 802.1x authentication > EAP Type menu on the device.
DOT1XID	String	Ethernet MAC Address of the device (\$MACA DDR) without the colon separators	Yes	Specifies the IEEE 802.1X Supplicant identifier for the Ethernet option. This parameter is supported in all modes. For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> file. - The Settings > Network > 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. This parameter is supported in all modes. For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> file. - The Settings > Network > Ethernet > IEEE 802.1x authentication > 802.1x credentials menu on the device.

Server addresses and ports

Parameter	Type	Default value	Is set to default on reset	Description
DNSSRV	String	0.0.0.0	Yes	Specifies up to three IP addresses of DNS servers in dot-decimal format.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				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 DNS servers in the order specified in the parameter. This parameter is supported in all modes. For provisioning, use: • The Option 6 value in a DHCPACK message. • The SET command in the <code>46xxsettings.txt</code> file. • The Settings menu on the device.
DOMAIN	String	Null	Yes	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. This parameter is supported in all modes. For provisioning, use: • The Option 15 value in a DHCPACK message. • The SET command in the <code>46xxsettings.txt</code> file.
FILE_SERVER_URL	String	Null	Yes	Specifies the configured 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: • <code>http://hostname[:port] [/path]</code> • <code>https://hostname[:port] [/path]</code> In the URL: • <code>hostname</code> is either an IP address in dotted-decimal format or a domain name.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				<code>port</code> is an optional port number. <code>path</code> is an optional path to a directory where distribution packages and other files are stored. Users can provide URLs of HTTP servers without the leading <code>http://</code>. Users must explicitly specify <code>https://</code> for HTTPS servers. The default port for HTTP is 80. The default port for HTTPS is 443. If this parameter is set, Avaya Vantage™ ignores the <code>HTTPSRVR</code>, <code>HTTPPORT</code>, <code>HTTPDIR</code>, <code>TLSSRVR</code>, <code>TLSSRVRDIR</code>, and <code>TLSPORT</code> parameters. This parameter is supported in all modes. For provisioning, use: - LLDP Avaya/Extreme Proprietary File Server TLV. The precedence is 1. - DHCP option 43. The precedence is 2. - A <code>name=value</code> pair in a DHCPACK message. The precedence is 2. - The <code>siaddr</code> field value in the DHCPACK message. The precedence is 2. Only the dot-decimal format is supported. Avaya Vantage™ considers addresses received using this method as HTTP server addresses. - The SET command in the <code>46xxsettings.txt</code> file. The precedence is 3. - The Settings menu on the device. The precedence is 5.
HTTPPROXY	String	Null	Yes	Specifies an address of an HTTP proxy server. A proxy server address uses the <code>hostname[:port]</code> format, where: <code>hostname</code> is either an IP address in the dot-decimal format or a domain name. <code>port</code> is an optional port number. This parameter is not a URL and it must not begin with <code>http://</code>. The range is the default string length. This parameter is supported in all modes.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> file. - The Settings menu on the device.
HTTPEXCEPTION DOMAINS	String	Null	Yes	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 to any domain specified in this parameter. This parameter is supported in all modes. For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> file. - The Settings menu on the device.
HTTPSRVR	String	0.0.0.0	Yes	Specifies a list of IP or DNS addresses of HTTP file servers for downloading firmware and configuration files. Avaya Vantage™ uses this parameter only if FILE_SERVER_URL and TLSSRV 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. This parameter is supported in all modes. For provisioning, use: - LLDP Avaya/Extreme Proprietary File Server TLV. The precedence is 1. - DHCP option 43. The precedence is 2. - A <code>name=value</code> pair in a DHCPACK message. The precedence is 2. - The <code>siaddr</code> field value in the DHCPACK message. The precedence is 2. Only the dot-decimal format is supported.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				The SET command in the <code>46xxsettings.txt</code> file. The precedence is 3.
TLSSVR	String	0.0.0.0	Yes	Specifies a list of IP or DNS addresses of HTTPS file servers for downloading firmware and configuration files. Avaya Vantage™ uses this parameter only if <code>FILE_SERVER_URL</code> 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. This parameter is supported in all modes. For provisioning, use: - LLDP Avaya/Extreme Proprietary File Server TLV. The precedence is 1. - DHCP option 43. The precedence is 2. - A <code>name=value</code> pair in a DHCPACK message. The precedence is 2.
HTTPDIR	String	Null	Yes	Specifies a path to the directory of the HTTP file server where configuration files and software images are stored. The path is relative to the root 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 <code>FILE_SERVER_URL</code> is not set. The parameter value can contain up to 127 characters. Do not use this parameter in configurations where files are stored in the default directory of the HTTP server. This parameter is supported in all modes. For provisioning, use: - A <code>name=value</code> pair in a DHCPACK message. - DHCP option 43. - The SET command in the <code>46xxsettings.txt</code> file.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
TLSDIR	String	Null	Yes	Specifies a path to the directory of the HTTPS file server where configuration files and software images are stored. The path is relative to the root of the HTTPS file server. Avaya Vantage™ prepends the parameter value to all file names used in HTTPS GET operations. Avaya Vantage™ uses this parameter only if FILE_SERVER_URL is not set. The parameter value can contain up to 127 characters. This parameter is supported in all modes. For provisioning, use: • A <code>name=value</code> pair in a DHCPACK message. • DHCP option 43. • The SET command in the <code>46xxsettings.txt</code> file.
HTTPPORT	Numeric	80	Yes	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. This parameter is supported in all modes. For provisioning, use: • A <code>name=value</code> pair in a DHCPACK message. • DHCP option 43. • The SET command in the <code>46xxsettings.txt</code> file.
TLSPORT	Numeric	443	Yes	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. This parameter is supported in all modes. For provisioning, use: • A <code>name=value</code> pair in a DHCPACK message. • DHCP option 43.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				The SET command in the <code>46xxsettings.txt</code> file.
SIP_CONTROLLE R_LIST	String	Null	Yes	Specifies a list of IP addresses of SIP proxy or registrar servers. The range is from 0 to 255. The value of the parameter is a list of SIP proxy server addresses separated by commas without any spaces between entries. Each entry in the list has the following format: <code>host[:port][;transport=xxx]</code>, where: <code>host</code> is an IP address in the dot-decimal or DNS format <code>port</code> is the optional port number. If you do not specify a port number, Avaya Vantage™ uses the following default values: - 5060 for TCP - 5061 for TLS <code>transport</code> is the optional transport type. The supported options are TLS or TCP. By default, Avaya Vantage™ uses the TLS transport type. The parameter value can have up to 255 characters. This parameter is <i>not</i> supported in the non Avaya Breeze™ CSDK application based mode. For provisioning, use: - LLDP Avaya/Extreme Proprietary Call Server TLV. The precedence is 1. - DHCP option 43. The precedence is 3. - A <code>name=value</code> pair in a DHCPACK message. The precedence is 3. - The SET command in the <code>46xxsettings.txt</code> file. The precedence is 4. - The value stored on the PPM or backup server. The precedence is 5. - The Settings menu on the device. The precedence is 5.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
SIPDOMAIN	String	Null	Yes	Specifies the SIP domain name used for SIP registration. The value of the parameter can have up to 255 characters. This parameter is <i>not</i> supported in the non Avaya Breeze™ CSDK application based mode. For provisioning, use: • The SET command in the <code>46xxsettings.txt</code> file. • The value stored on the PPM server. • The Settings menu on the device.
SNTPSRVR	String	Null	Yes	Specifies a list of addresses of Simple Network Time Protocol (SNTP) servers. 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 addresses using either the dot-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. This parameter is supported in all modes. For provisioning, use: • DHCP option 42. • The SET command in the <code>46xxsettings.txt</code> file.
LOGSRVR	String	Null	Yes	Specifies an address of a server where syslog messages are stored. LOGSRVR can store one IP address of the syslog server in the dot-decimal or DNS format. The parameter value can have up to 255 characters. This parameter is supported in all modes. For provisioning, use: • DHCP option 7 in a DHCPACK message. • The Settings menu on the device.
USER_AUTH_FILE_SERVER_URL	String	Null	Yes	Specifies a list of user authenticated file server URLs. • If this parameter is configured, Avaya Vantage™ displays the Unified Login screen. In the current

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				release, Avaya Vantage™ supports Avaya Aura® Device Services user authentication servers only. If you did not provide the user's SIP extension and password in the Avaya Aura® Device Services, Avaya Vantage™ will also prompts the user to enter the SIP extension and password. - If this parameter is not configured, Avaya Vantage™ displays the SIP login screen. In this case, the user only need 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 one of the following formats: <code>http://hostname[:port]</code> <code>https://hostname[:port]</code> In the URL: <code>hostname</code> is either an IP address in dot-decimal format or a domain name. <code>port</code> is an optional port number. Users can provide URLs of HTTP servers without leading <code>http://</code>. Users must explicitly specify <code>https://</code> for HTTPS servers. The default port for HTTP is 80. The default port for HTTPS is 443. This parameter is supported in all modes. For provisioning, use: - A <code>name=value</code> pair in a DHCPACK message. - The SET command in the <code>46xxsettings.txt</code> file. - The Settings menu on the device.

Other operational parameters and settings

The following sections describe configuration parameters that control Avaya Vantage™ behavior, but do not relate to network operations or UI appearance.

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 Breeze™ CSDK 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 Breeze™ CSDK application, such as Avaya Equinox™ or Avaya Vantage™ Basic. Otherwise, this parameter must use the default value. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

Third party applications

Parameter	Type	Default value	Is set to default on reset	Description
PUSH_APPLICATION	String	null string	Yes	Specifies a list of third party applications that administrators define for installation on Avaya Vantage™. Each entry of 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 <code>http://</code> or <code>https://</code>.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> 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 <code>FILE_SERVER_URL</code> or <code>HTTPDIR</code> and <code>TLSDIR</code> parameters depending on whether the download uses HTTP or HTTPS • Absolute path format. In this case, the URL must begin with <code>http://</code> or <code>https://</code> This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
USER_INSTALL_APPS_GOOGLE_PLAY_STORE	Numeric	0	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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
PIN_APP	String	null string	Yes	Specifies the package name of the application that must be pinned. If this parameter is configured and the specified application is installed, Avaya Vantage™ shows this application after login. Users cannot switch to another applications or navigate to the Home screen. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

Dial plan parameters

Parameter	Type	Default value	Is set to default on reset	Description
PHNEMERGNUM	String	Null string	Yes	Specifies the emergency number. Avaya Vantage™ dials this number when uses taps Emergency call. The parameter value can contain up to 30 characters. You can use 0–9, *, and # characters. This parameter is <i>not</i> supported in the non Avaya Breeze™ CSDK application based mode. For provisioning, use PPM.
PHNMOREEMERGENUMS	String list	Null string	Yes	Specifies additional 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 <i>not</i> supported in the non Avaya Breeze™ CSDK application based mode. For provisioning, use PPM.

Protocol-specific parameters

Certificates configuration parameters

Parameter	Type	Default value	Is set to default on reset	Description
TRUSTCERTS	String	null string	Yes	Specifies file names of trusted certificates which are used for authentication. 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 symbols. Avaya Vantage™ supports both the PEM and DER file formats. This parameter is supported in all modes.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
MYCERTURL	String	null string	Yes	Specifies a URL of the Simple Certificate Enrollment Protocol (SCEP) server. Avaya Vantage™ attempts to contact the server if the parameter value is not default. A valid URL must start with <code>http://</code>. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
MYCERTCN	String	\$SERIALNO	Yes	Specifies the Common Name (CN) for SUBJECT in a SCEP certificate request. If the parameter value contains the <code>\$SERIALNO</code> string, Avaya Vantage™ replaces this string with the device serial number. If the parameter value contains the <code>\$MACADDR</code> string, Avaya Vantage™ replaces that string with the device MAC address. * Note: The parameter value must not contain the <code>*</code> symbol. If the parameter value contains this symbol, Avaya Vantage™ considers the value to be invalid. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> 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 (<code>/</code>) symbol. * Note: The parameter value must not contain the <code>*</code> symbol. If the parameter value contains this symbol, Avaya Vantage™ considers the value to be invalid.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				For example: /C=US/ST=CA/L=MILPITAS/O=Avaya This parameter is supported in all modes. For provisioning, use the SET command in the <code>46xxsettings.txt</code> file.
MYCERTKEYLEN	Integer	2048	Yes	Specifies the RSA private key length in bits. The private key is used on the device for a certificate enrollment. Avaya Vantage™ only supports keys with the length of 2048 bits. This parameter is supported in all modes. For provisioning, use the SET command in the <code>46xxsettings.txt</code> 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. This parameter is supported in all modes. For provisioning, use the SET command in the <code>46xxsettings.txt</code> 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. This parameter is supported in all modes. For provisioning, use: • The SET command in the <code>46xxsettings.txt</code> 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

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> 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 revoke or if you do not trust the certificate. Add only certificates which are not already disabled in Android. You can find the list of these certificates in the <code>/data/misc/keychain/pubkey_blacklist.txt</code> file. This parameter can contain up to 1024 characters. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file. For example: <code>SET CA_CERT_BLACKLIST 410f36363258f30b347d12ce4863e433437806a8,c4f9663716cd5e71d6950b5f33ce041c95b435d1</code>
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: • <code>\$SERIALNO</code>: This options is replaced with the Avaya Vantage™ serial number • <code>MACADDR</code>: 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 <code>http://<path_to_the_file>/pkc12file_</code>

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				\$MACADDR.cer. In this case, the PKCS file for the device must have the <code>pkc12file_0024D7E42E98</code> name. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
PKCS12PASSWORD	String	Null	Yes	Specifies a PKCS #12 file password. This parameter is supported in all modes. For provisioning, use: • The SET command in the <code>46xxsettings.txt</code> file. • The Settings menu on the device.
PKCS12_PASSWORD_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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
CERT_INSTALL_APPLICATION_LIST	String	all	Yes	Specifies which applications can install trusted and identity certificates on Avaya Vantage™. Assign one of the following values: • all: All applications can install certificates. • Null string: No application can install certificates. • A list of comma-separated application package names: Only the specified applications can install certificates. List entries are separated by commas. For example: <code>SET CERT_INSTALL_APPLICATION_LIST flare.avaya.com,vantage.basic.avaya.com</code> For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
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 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 CERT_INSTALL_APPLICATION_LIST flare.avaya.com,vantage.basic.avaya.com This parameter is supported in all modes. 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. This parameter is supported in all modes. 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.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> 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 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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> 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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

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 <code>[http://]hostname[:port][/path]</code> format, where: <code>hostname</code> is either an IP address in dot-decimal format or a domain name. <code>port</code> is an optional port number. <code>path</code> is an optional path to the server. If you want to disable the detection mechanism, use the null string as the parameter value.

Parameter	Type	Default value	Is set to default on reset	Description
				This parameter is supported in all modes. For provisioning, use: - DHCP option 242. - The SET command in the <code>46xxsettings.txt</code> 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. This parameter is supported in all modes. For provisioning, use: - DHCP option 43. - The SET command in the <code>46xxsettings.txt</code> file.
TLS_VERSION	Numeric	0	Yes	Specifies which TLS versions are supported with all TLS connections used by Android and AvayaAvaya 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. This parameter is supported in all modes. For provisioning, use the SET command in the <code>46xxsettings.txt</code> 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.

Parameter	Type	Default value	Is set to default on reset	Description
				• 1: Enabled. • 2: Enabled. Avaya Vantage™ starts to transmit LLDP frames only after receiving of an LLDP frame. This parameter is supported in all modes. For provisioning, use the SET command in the <code>46xxsettings.txt</code> file.

Logging and debugging parameters

Parameter	Type	Default value	Is set to default on reset	Description
SYSLOG_ENABLE D	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. This parameter is supported in all modes. For provisioning, use: • The SET command in the <code>46xxsettings.txt</code> 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 This parameter is supported in all modes. For provisioning, use: • The SET command in the <code>46xxsettings.txt</code> file.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				The Settings menu on the device.
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 storage is enabled. This parameter is supported in all modes. For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> 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 This parameter is supported in all modes. For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> file. - The Settings menu on the device.
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 level 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.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				- 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. This parameter is supported in all modes. For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> file. - The Settings menu on the device.
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. This parameter is supported in all modes. For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> 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. This parameter is supported in all modes. For provisioning, use the SET command in the <code>46xxsettings.txt</code> 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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
SSH_ROOT_ALLOWED	Numeric	1	Yes	Specifies whether root access is allowed. Assign one of the following values: • 0: root access is disabled. • 1: root access is enabled. This parameter is supported in all modes. For provisioning, use: • The <code>SET</code> command in the <code>46xxsettings.txt</code> file. • The Settings menu on the device.

USB parameters

Parameter	Type	Default value	Is set to default on reset	Description
ENABLE_USB_GENERAL_PURPOSE	Numeric	1	Yes	Specifies if the USB general purpose port is enabled. Assign one of the following values: • 0: USB port is disabled. • 1: USB port is enabled. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file. PPM does not back up or restore the parameter.

Upgrade related parameters

Upgrade related parameters

Parameter	Type	Default value	Is set to default on reset	Description
UPGRADE_POLLING_PERIOD	Integer	60	Yes	Specifies the polling interval between two consecutive attempt of polling both firmware image and settings file. The polling interval is measured in minutes. Assign one of the following values: • 0: Disabled • 1–10080: Enabled This parameter is supported by ADVD (with the range of 0– 65535). This parameter has no effect on any upgrade command that is triggered by the management application or UI. UPGRADE_POLLING_PERIOD is not affected by UPGRADE_DLOAD_START and UPGRADE_DLOAD_END parameters. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
UPGRADE_DLOAD_START	String	00	Yes	Specifies a time when Avaya Vantage™ starts to download upgrade image files. The value of parameter is a string in the <code>[Ddd]hh</code> format, where: • <code>[Ddd]</code> is a day of the week. The valid values are <code>Sun</code>, <code>Mon</code>, <code>Tue</code>, <code>Wed</code>, <code>Thu</code>, <code>Fri</code>, or <code>Sat</code>. This component is optional. If the component is omitted, Avaya Vantage™ performs polling every day. • <code>hh</code> is one or two numeric digits representing a 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 is ignored if UPGRADE_POLICY is set to 0. This parameter is supported in all modes.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
UPGRADE_DLOAD_END	String	00	Yes	Specifies a time when Avaya Vantage™ stops tries to download upgrade image files. The value of the parameter uses the <code>[Ddd]hh</code> format, where: <code>[Ddd]</code> 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. <code>hh</code> is one or two numeric digits representing a hour of the day. The range is from 0 to 23. If the <code>UPGRADE_DLOAD_START</code> value is equal to the <code>UPGRADE_DLOAD_END</code> value, then no polling period is specified and Avaya Vantage™ can download upgrade files at any time. <code>UPGRADE_DLOAD_END</code> is ignored if <code>UPGRADE_POLICY</code> is set to 0. Avaya Vantage™ completes any ongoing downloads if time specified in <code>UPGRADE_DLOAD_END</code> is reached when downloading files. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
UPGRADE_INSTALL_DATE_TIME	String	1970-01-01T00:00	Yes	Specifies the date and time when Avaya Vantage™ starts to install upgrade files. The value of the parameter uses the <code>YYYY-MM-DDThh:mm</code> format, where: <code>YYYY</code> is four numeric digits representing the year <code>MM</code> is two numeric digits representing the month. <code>dd</code> is two numeric digits representing the day of the month. <code>T</code> is a time separator. <code>hh</code> is two numeric digits representing a hour of the day. The range is from 0 to 23. <code>mm</code> is two numeric digits representing minutes of the hour. The range is from 0 to 59.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				If the default value is used, Avaya Vantage™ installs upgrades immediately after downloading. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
UPGRADE_POLICY	Integer	2	Yes	Specifies the upgrade policy. Assign one of the following values: • 0: Avaya Vantage™ performs upgrade procedure after reboot only. If the upgrade configuration policy is changed, Avaya Vantage™ implements these changes after reboot. • 1: Avaya Vantage™ performs upgrade procedure according to policy rules and management application settings. Avaya Vantage™ does not perform upgrade procedure after reboot. • 2: Avaya Vantage™ performs upgrade procedure after any reboot and according to policy rules and management application settings. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
DLOAD_RND_AFTER_RESET	Integer	0	Yes	Specifies the maximum length of an interval Avaya Vantage™ waits after reboot before starting the download. 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 <code>DLOAD_RND_AFTER_RESET</code> value. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
DLOAD_RND	Integer	3600	Yes	Specifies the maximum length of an interval between two consecutive attempts of background

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				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. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

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 <i>not</i> supported in the non Avaya Breeze™ CSDK application based mode. For provisioning, use: • Enter the user account name on the Login screen. • Use the <code>SET</code> command in the settings file from AADS. The <code>46xxsettings.txt</code> file from the HTTP or HTTPS server is not supported.
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 <i>not</i> supported in the non Avaya Breeze™ CSDK application based mode. For provisioning: • Enter the user account name on the Login screen.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				Use the SET command in the settings file from Avaya Aura[®] Device Services. The <code>46xxsettings.txt</code> file from the HTTP or HTTPS server is <i>not</i> 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 alphanumeric characters. This parameter is <i>not</i> supported in the non Avaya Breeze[™] CSDK application based mode. This parameter is only configurable from Avaya Aura[®] Device Services. The <code>46xxsettings.txt</code> file from the HTTP or HTTPS server is <i>not</i> supported.
PROCPSWD	String	27238	Yes	Specifies the password required to access local administrator menus on Avaya Vantage[™]. The parameter value can contain from 4 to 7 numeric characters. If both PROCPSWD and ADMIN_PASSWORD have default values, you cannot access administrator options in the Settings application. This parameter is supported in all modes. For provisioning, use: - A <code>name=value</code> pair in a DHCPACK message. - The SET command in the <code>46xxsettings.txt</code> file. - The value stored on the PPM server.
ADMIN_PASSWORD	String	Null	Yes	Specifies the complex password required to access administrator menus on Avaya Vantage[™]. The range is the default string length. - 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 menus. If PROCPSWD has the default value, you cannot access administrator menus.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				This parameter is supported in all modes. For provisioning, use the SET command in the <code>46xxsettings.txt</code> file. This parameter is supported in the Tablet mode.
ALLOW_LOGOUT_WHEN_LOCKED	Numeric	1	Yes	Specifies whether users can log out from the Lock screen. Assign one of the following values: • 0: Users cannot perform logout when the device is locked. • 1: User can perform logout from the Lock screen. • 2: Only administrators can perform logout procedure. Logout procedure is performed using the Settings application. Only administrators can force user logout when a user is logged in to the device and the device is not locked. The logout option shall not be presented for administrator when the device is logout. For provisioning, use • The SET command in the <code>46xxsettings.txt</code> file. • The settings file received from AADS.

Phone lock parameters

Parameter	Type	Default value	Is set to default on reset	Description
ENABLE_PHONE_LOCK	Numeric	0	No	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 <i>not</i> supported in the non Avaya Breeze™ CSDK application based mode. For provisioning, use: • The SET command in the <code>46xxsettings.txt</code> file. • The Settings menu on the device.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
PHONE_LOCK_IDLETIME	Numeric	60	No	Specifies the maximum idle time interval in minutes after which Avaya Vantage™ becomes locked. Avaya Vantage™ uses this parameter to determine the number of options it shows to the user in the Settings > Security > Lock screen message menu. By default, this menu has 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 determined as 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 Lock screen message menu will contain values from 1 minute to 2 hours inclusively. Avaya Vantage™ ignores this parameter if ENABLE_PHONE_LOCK is 0. The range is from 1 to 10080. This parameter is <i>not</i> supported in the non Avaya Breeze™ CSDK application based mode. For provisioning, use the SET command in the 46xxsettings.txt file.
PHONE_LOCK_PASSWORD_FAILED_ATTEMPTS	Numeric	8	Yes	Specifies the number of failed attempts to log in 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 <i>not</i> supported in the non Avaya Breeze™ CSDK application based mode. For provisioning, use the SET command in the 46xxsettings.txt file.
LOCK_SCREEN_LOCK_AFTER_TIMEOUT	Numeric	5	Yes	Specifies the Lock screen inactivity timeout in minutes. The range is from 1 to 10080. This parameter is <i>not</i> supported in the non Avaya Breeze™ CSDK application based mode. For provisioning, use the Settings menu on the device.

Security parameters

Parameter	Type	Default value	Is set to default on reset	Description
SELINUX_MODE	Numeric	1	N/A	Sets the SELinux mode. • 0: Sets the permissive mode. • 1: Sets the enforcing mode. ! Important: It is recommended to use the permissive mode. This parameter is supported in all modes. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

Avaya Breeze™ CSDK parameters

The following parameters are supported by Avaya Breeze™ CSDK-based applications.

Avaya Aura® Device Services parameters

Parameter	Type	Default value	Is set to default on reset	Description
ACSENABLED	Numeric	0	Yes	Specifies whether Avaya Vantage™ Basic uses contacts stored on Avaya Aura® Device Services. Assign one of the following values: • 0: Avaya Vantage™ Basic uses contacts stored on Avaya Aura® Device Services. Avaya Vantage™ Basic does not use PPM contacts. • 1: Avaya Vantage™ Basic does not use contacts stored on Avaya Aura® Device Services. Avaya Vantage™ Basic uses PPM contacts. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
ACSSVR	String	Null string	Yes	Specifies the address of Avaya Aura® Device Services contact services. The address is either an IP address in the dot-decimal format or a domain name.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
ACSPORT	Numeric	443	Yes	Specifies the port number Avaya Vantage™ Basic uses to connect to Avaya Aura® Device Services contact services. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
ACSSECURE	Numeric	1	Yes	Specifies whether a secure connection is used. Assign one of the following values: • 0: Secure connection is not used. Avaya Vantage™ Basic uses HTTP over TCP. • 1: Secure connection is used. Avaya Vantage™ Basic uses HTTPS over TLS. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

SIP parameters

Parameter	Type	Default value	Is set to default on reset	Description
RTP_PORT_LOW	Numeric	5004	Yes	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 <code>SET</code> command in the <code>46xxsettings.txt</code> file.
RTP_PORT_RANGE	Numeric	40	Yes	Specifies the UDP port range that Avaya Vantage™ Basic 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 <code>RTP_PORT_LOW</code> and <code>RTP_PORT_RANGE</code> values. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

S RTP parameters

Parameter	Type	Default value	Is set to default on reset	Description
MEDIAENCRYPTION	String	1,2,9	Yes	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 <code>SET</code> command in the <code>46xxsettings.txt</code> file.
ENCRYPT_SRTCP	Numeric	0	Yes	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 <code>SET</code> command in the <code>46xxsettings.txt</code> file.

Audio parameters

Parameter	Type	Default value	Is set to default on reset	Description
ENABLE_OPUS	Numeric	1	Yes	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 NARROWBAND_12K. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
OPUS_PAYLOAD_TYPE	Numeric	116	Yes	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.

Video parameters

Parameter	Type	Default value	Is set to default on reset	Description
VIDEO_MAX_BANDWIDTH_ANY_NETWORK	Numeric	128	Yes	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 <code>46xxsettings.txt</code> file.

Logging parameters

Parameter	Type	Default value	Is set to default on reset	Description
LOG_VERBOSITY	Numeric	0	Yes	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.

Dialing rule parameters

Parameter	Type	Default value	Is set to default on reset	Description
ENHDIALSTAT	Numeric	1	Yes	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: For Avaya Vantage™ Basic. • 1: For CSDK-based applications.	Yes	Specifies the country code. Valid values are from 1 to 999.
PHNIC	String	• Null string: For Avaya Vantage™ Basic. • 011: For CSDK-based applications.	Yes	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: For Avaya Vantage™ Basic. • 1: For CSDK-based applications. 1	Yes	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: For Avaya Vantage™ Basic. • 5: For CSDK-based applications.	Yes	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.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
PHNLDLENGTH	String	- Null string: For Avaya Vantage™ Basic. 10: For CSDK-based applications.	Yes	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: For Avaya Vantage™ Basic. 9: For CSDK-based applications.	Yes	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	Yes	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. Whenever possible, configure the plus (+) dialing option in Session Manager instead of enabling this parameter.
AUTOAPPLY_ARS_TO_SHORTNUMBERS	Numeric	1	Yes	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	Is set to default on reset	Description
PHNREMOVEAREACODE	String	0	Yes	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 you to use the newer parameter, DIALPLANLOCALCALLPREFIX.
DIALPLANLOCALCALLPREFIX	String	0	Yes	Indicates whether the area code must be removed for local calls. Assign one of the following values: • 0: To disable the removal of area code for local calls. • 1: To enable the removal of area code for local calls.  Note: Area code is configured using DIALPLANAREACODE.
DIALPLANNATIONALPHONENUMLENGTHLIST	String	Null string	Yes	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	Yes	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	Yes	Specifies the PBX main prefix.
PHNPBXMAINPREFIX	String	Null string	Yes	Specifies the PBX main prefix. This parameter is obsolete. While it is still supported for backward compatibility, Avaya

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				recommends you to use the newer parameter, DIALPLANPBXPREFIX.
DIALPLANAREACODE	String	Null string	Yes	Specifies the area or city code.
SP_AC	String	Null string	Yes	Specifies the area or city code. This parameter is obsolete. While it is still supported for backward compatibility, Avaya recommends you to use the newer parameter, DIALPLANAREACODE.

Avaya Vantage™ Basic parameters

Layer 3 QoS parameters

Parameter	Type	Default value	Is set to default on reset	Description
DSCPAUD	Numeric	46	Yes	Specifies the decimal presentation of Differentiated Services Code Point (DSCP) for audio frames generated by the device. You can assign a value between 0 and 63. For provisioning, use: • The SET command in the <code>46xxsettings.txt</code> file. The precedence is 3. • The TIA LLDP MED Network policy TLV. The precedence is 4.
DSCPSIG	Numeric	34	Yes	Specifies the decimal presentation of DSCP for signaling frames generated by the device. You can assign a value between 0 and 63. For provisioning, use: • The SET command in the <code>46xxsettings.txt</code> file. The precedence is 3. • The TIA LLDP MED Network policy TLV. The precedence is 4.
DSCPVID	Numeric	34	Yes	Specifies the decimal presentation of DSCP for video frames generated by the device.

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				You can assign a value between 0 and 63. For provisioning, use: - The SET command in the <code>46xxsettings.txt</code> file. The precedence is 3. - The TIA LLDP MED Network policy TLV. The precedence is 4.

Call option parameters

Parameter	Type	Default value	Is set to default on reset	Description
ENABLE_REDIAL	Numeric	1	Yes	Specifies whether the Redial button is available to users. 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 <code>46xxsettings.txt</code> file.
CCBTNSTAT	Numeric	1	Yes	Specifies whether you can enable or disable the conferencing, call transfer, call hold, and mute features separately using the corresponding parameters. Assign one of the following values: 0: Avaya Vantage™ Basic uses the values of parameters related to these features. You can configure the availability of each feature separately. 1: Avaya Vantage™ Basic 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

Table continues...

Parameter	Type	Default value	Is set to default on reset	Description
				For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
HOLDSTAT	Numeric	1	Yes	Specifies whether the Hold button is available to users. Avaya Vantage™ Basic 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 <code>SET</code> command in the <code>46xxsettings.txt</code> file.
MUTESTAT	Numeric	1	Yes	Specifies whether the Mute button is available to users. This option controls muting for both audio and video. Avaya Vantage™ Basic ignores this parameter if CCBTNSTAT is set to 1. Assign one of the following values: • 0: The Mute button is disabled. • 1: The Mute button is enabled. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
CONFSTAT	Numeric	1	Yes	Specifies whether the Conference button is available to users. Avaya Vantage™ Basic ignores this parameter if CCBTNSTAT is set to 1. Assign one of the following values: • 0: The Conference button is disabled. • 1: The Conference button is enabled. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
XFERSTAT	Numeric	1	Yes	Specifies whether the Call transfer button is available to users. Avaya Vantage™ Basic ignores this parameter if CCBTNSTAT is set to 1. Assign one of the following values: • 0: The Call transfer button is disabled. • 1: The Call transfer button is enabled. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

Audio parameters

Parameter	Type	Default value	Is set to default on reset	Description
ADMIN_CHOICE_RINGTONE	String	Default	Yes	Specifies the ring tone that Avaya Vantage™ Basic uses for incoming calls. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

Contact parameters

Parameter	Type	Default value	Is set to default on reset	Description
ENABLE_MODIFY_CONTACTS	Numeric	1	Yes	Specifies whether users can modify contacts. Assign one of the following values: • 0: Users cannot modify contacts. • 1: Users can modify contacts. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
NAME_SORT_ORDER	String	last,first	Yes	Specifies how contact names are sorted. You can assign one of the following values: • last,first: Avaya Vantage™ Basic sorts contacts according to the last name and then according to the first name. • first,last: Avaya Vantage™ Basic sorts contacts according to the first name and then according to the last name. For example: <code>SET NAME_SORT_ORDER "first,last"</code> . For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.
NAME_DISPLAY_ORDER	Numeric	0	Yes	Specifies how contact names are displayed. You can assign one of the following values: • 0: Avaya Vantage™ Basic displays the last name followed by the first name. • 1: Avaya Vantage™ Basic displays the first name followed by the last name. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

Display parameters

Parameter	Type	Default value	Is set to default on reset	Description
BRANDING_FILE	String	null string	Yes	Specifies the URL of a branding image. Avaya Vantage™ Basic 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 <code>http://</code> or <code>https://</code>. The image must use the following settings: • Resolution: 142x56. • File format: PNG, JPG, JPEG, GIF, or BMP. For provisioning, use the <code>SET</code> command in the <code>46xxsettings.txt</code> file.

Appendix B: Unsupported configuration parameters

The following configuration parameters are not supported by Avaya Vantage™.

Name	Supported on 96xx phones	Supported on H175
1XP_SERVER_ADDR	—	Y
ADDITIONAL_FORWARDING_FEATURES	Y	—
ADMIN_HSEQUAL	Y	—
AGENT_NOT_LOGGED_IN	Y	—
AGENTTONE	Y	—
ALLOW_DND_SAC_LINK_CHANGE	Y	—
AMADMIN	Y	—
AST_FEATURE_TIMEOUT_VALUE	—	Y
ASTCONFIRMATION	—	Y
AUDIOENV	—	Y
AUDIOZERODBM	Y	—
AUTO_SELECT_ANY_IDLE_APPR	Y	—
AWAY_PRESENCE_OPTIMIZATIONS	—	Y
BCA_BUTTON_RING_TYPE_PER_BUTTON	Y	—
BLOCK_OUTGOING_VIDEO_ANSWER_MODE	—	Y
BOOT1INUSE	Y	—
BOOTNAME	Y	—
BRIGHTNESS	Y	—
BUTTON_MAPPINGS	Y	—
CALL_LOG_PERSISTENT	Y	—
CALL_TRANSFER_MODE	Y	—
CALENDAR_HOST_CODE_STRING	—	Y
CALENDAR_MEETING_ID_STRING	—	Y

Table continues...

Name	Supported on 96xx phones	Supported on H175
CALENDAR_MEETING_PIN_STRING	—	Y
CALENDAR_PARTICIPANT_CODE_STRING	—	Y
CALENDAR_PHONE_NUM_MIN_DIGITS	—	Y
CALENDAR_PREFERENCES	—	Y
CALLFWDADDR	Y	—
CALLFWDALL_ACTIVE	Y	—
CALLFWDALL_ADDR	Y	—
CALLFWDDBUSY_ACTIVE	Y	—
CALLFWDDBUSY_ADDR	Y	—
CALLFWDDELAY	Y	—
CALLFWDNOANS_ACTIVE	Y	—
CALLFWDNOANS_ADDR	Y	—
CALLFWDSTAT	Y	—
CC_INFO_TIMER	Y	—
CF_RINGTONE	Y	—
CLDISPCONTENT	Y	—
CLONE_DISPLAY	—	Y
CNAPORT	Y	—
CNASRVR	Y	—
CNASRVR_IN_USE	Y	—
CNGLABEL	Y	—
CODECR	Y	—
CODECT	Y	—
CONF_TRANS_ON_PRIMARY_APPR	Y	—
CONFERENCE_BLUEPRINT_INFO	Y	—
CONFERENCE_FACTORY_URI	—	Y
CONFERENCE_SERVER_ADDRESS	Y	—
CONFERENCE_SERVER_PORT	Y	—
CONFERENCE_SERVICE_ADDRESS	Y	—
CONFERENCE_TYPE	Y	—
CONFIG_FQD_HOST_NAME	—	Y
CONFIG_SERVER	—	Y
CONFIG_SERVER_SECURE_MODE	—	Y
CONNECTION_REUSE	—	Y

Table continues...

Name	Supported on 96xx phones	Supported on H175
CONTINUOUS_SCROLLING	Y	—
CONTRAST	Y	—
CONTROLLER_SEARCH_INTERVAL	—	Y
COVERAGEADDR	Y	—
CRAFT_MENU_DISPLAY_AST_OPTION	Y	—
CURRENT_CONTENT	Y	—
CURRENT_LOGO	Y	—
CURRENT_PHONE_LANGUAGE	Y	—
CURRENT_SKIN	Y	—
DATEFORMAT	Y	—
DAYLIGHT_SAVING_SETTING_MODE	—	Y
DECTSTAT	—	Y
DELAYED_INIT_AFTER_LINK_RECOVERY_TIMER_MSEC	Y	—
DHCP_CHADDR	Y	—
DIALPLAN	—	Y
DISCOVER_AVAYA_ENVIRONMENT	—	Y
DISPLAY_NAME_NUMBER	Y	—
DLOAD_RETRY	—	Y
DOT1X	—	Y
DSTOFFSET	—	Y
DSTSTART	—	Y
DSTSTOP	—	Y
DYNAMIC_VIDEO_SIZE_REQUEST	—	Y
DYNAMIC_VIDEO_SIZE_REQUEST_DELAY	—	Y
DND_SAC_LINK_MANUAL	Y	—
E2E_SECURE_CALL	—	Y
ENABLE_APPS	—	Y
ENABLE_AUDIO_BRAND	Y	—
ENABLE_AVAYA_ENVIRONMENT	—	Y
ENABLE_BLUETOOTH	—	Y
ENABLE_CALL_LOG	Y	—
ENABLE_CONTACTS_AUTODIAL	—	Y
ENABLE_DECT	—	Y
ENABLE_EARLY_MEDIA	—	Y

Table continues...

Name	Supported on 96xx phones	Supported on H175
ENABLE_EXCHANGE_REMINDER	Y	—
ENABLE_FIR	—	Y
ENABLE_G711A	—	Y
ENABLE_G711U	—	Y
ENABLE_G722	—	Y
ENABLE_G726	—	Y
ENABLE_G729	—	Y
ENABLE_HOLD_BUTTON	Y	—
ENABLE_IPOFFICE	—	Y
ENABLE_MEDIA_CONTROLS	—	Y
ENABLE_MODIFY_CONTACTS	Y	—
ENABLE_MULTIPLE_CONTACTS_WARNING	Y	—
ENABLE_OOD_MSG_TLS_ONLY	—	Y
ENABLE_PLI	—	Y
ENABLE_PPM_SOURCED_SIPPROXYSRVR	—	Y
ENABLE_PRESENCE	—	Y
ENABLE_REDIAL_LIST	Y	—
ENABLE_REMOVE_PSTN_ACCESS_PREFIX	—	Y
ENABLE_SDCARD	—	Y
ENABLE_SECURE_HTTP_FOR_CONFERENCING_SERVICE	Y	—
ENABLE_SERVER_BASED_PRESENCE	Y	—
ENABLE_SHOW_EMERG_SK	Y	—
ENABLE_SHOW_EMERG_SK_UNREG	Y	—
ENABLE_SIP_USER_ID	Y	—
ENABLE_TMMBR	—	Y
ENABLE_WIFI	—	Y
ENFORCE_DVI	—	Y
ENTRYNAME	Y	—
ERRORTONE	Y	—
EVENT_NOTIFY_AVAYA_MAX_USERS	Y	—
EXCHANGE_EMAIL_DOMAIN	Y	—
EXCHANGE_NOTIFY_SUBSCRIPTION_PERIOD	Y	—
EXCHANGE_REMINDER_TIME	Y	—
EXCHANGE_REMINDER_TONE	Y	—

Table continues...

Name	Supported on 96xx phones	Supported on H175
EXCHANGE_SERVER_IN_USE	Y	—
EXCHANGE_SERVER_MODE	Y	—
EXCHANGE_SNOOZE_TIME	Y	—
EXTEND_RINGTONE	Y	—
EXTERNAL_APP_INTERFACE_PORT	Y	—
EXTERNAL_APP_INTERFACE_STATUS	Y	—
EXTERNAL_APP_INTERFACE_TRANSPORT_TYPE	Y	—
FAILBACK_POLICY	—	Y
FAILED_SESSION_REMOVAL_TIMER	—	Y
FAST_RESPONSE_TIMEOUT	—	Y
FAVORITES	Y	—
FEIPADD	—	Y
FEPOR	—	Y
FEPORVID	—	Y
FONT_IN_USE	Y	—
HEADSYS	Y	—
GMTOFFSET	—	Y
HOMEIDLETIME	Y	—
HOTLINE	—	Y
HSEQUALIZATION	Y	—
IM_ALERT_TONE	Y	—
INBOUND_SUBSCRIPTION_GRANT_DURATION	—	Y
INPUT_METHOD	Y	—
INSTANT_MSG_ENABLED	Y	—
INTER_DIGIT_TIMEOUT	—	Y
IPO_FULL_USERNAME	—	Y
IPO_SUPPORTED_HEADER_OPTION_PARAMETER	—	Y
IPO_USERNAME	—	Y
JMSEC	Y	—
KEY_LAYOUT_FILES	—	Y
LANG0STAT	Y	—
LANGLARGFONT	Y	—
LANGUAGE_DIRECTION	Y	—
LANGUAGE_FILE_IN_USE	Y	—

Table continues...

Name	Supported on 96xx phones	Supported on H175
LANGUAGES_RESOURCE_LIST	Y	—
LINE_RESERVATION_TIMER	—	Y
LOCAL_CONFERENCE_MODE	—	Y
LOCAL_DIAL_AREA_CODE	—	Y
LOCAL_PRESENCE_UPDATE_DELAY_TIMER_MSEC	Y	—
LOCALLY_ENFORCE_PRIVACY_HEADER	—	Y
LOGOS	Y	—
LP_HSEQUAL	Y	—
MATCHTYPE	Y	—
MAX_CALL_LOG_ENTRIES	Y	—
MAX_CONTACTS_ENTRIES	Y	—
MAX_LOCAL_CONFERENCE_PARTIES	Y	—
MAX_NUM_CONFERENCE_RESOURCES	Y	—
MUSICSRVR	Y	—
MUSICSRVR_IN_USE	Y	—
MUTE_ON_REMOTE_OFF_HOOK	—	Y
MWISVR	—	Y
MWISVR_IN_USE	Y	—
MYCERTRENEW	—	Y
NETWORK_PROGRESS_TONE_HANDSET_LEVEL	Y	—
NETWORK_PROGRESS_TONE_HEADSET_LEVEL	Y	—
NETWORK_PROGRESS_TONE_SPEAKER_LEVEL	Y	—
NETWORK_RECOVERY_ATTEMPT_MAX_DELAY	—	Y
NETWORK_RECOVERY_ATTEMPT_MIN_DELAY	—	Y
NO_DIGITS_TIMEOUT	—	Y
NON_PERSISTANT_EXCHANGE_USER_ACCOUNT	Y	—
NON_PERSISTANT_EXCHANGE_USER_PASSWORD	Y	—
OFFLINE_USER_PERIODIC_QUERY_TIMER	Y	—
OFFLINE_USER_TO_POLL_LIMIT	Y	—
OPTHOMEIDLE	Y	—
OPTTEXTSIZE	Y	—
OUTBOUND_SUBSCRIPTION_REQUEST_DURATION	—	Y
OUTGOING_CALL_MODE	—	Y
P_CONF_FEEDBACK_PROMPTS	—	Y

Table continues...

Name	Supported on 96xx phones	Supported on H175
P_CONF_OUTDIAL_PROMPT	—	Y
PERIODIC_CHECK_FOR_AST_FEATURE_TIMEOUT	—	Y
PERIODIC_PRESENCE_LIST_TIMEOUT	Y	—
PERSONALRING	Y	—
PHNDSPLYALERT	Y	—
PHNLAC	—	Y
PHNMUTEALERT	Y	—
PHNMUTEALERT_BLOCK	Y	—
PHNNUMOFSA	—	Y
PHNQUICKPANEL	Y	—
PHNSCRONALERT	Y	—
PHNSCRONCALL	Y	—
PHNSCRWIDTH	Y	—
PHNTIMERS	Y	—
PHNVISUALALERT	Y	—
PHONE_SCREEN_EXT_URL	Y	—
PHY1DUPLEX	Y	—
PHY2DUPLEX	Y	—
PHY2_AUTOMDIX_ENABLED	—	Y
PHY2_OPERATIONAL_MODE	—	Y
PHY2PRIO	Y	—
PHY2STAT	—	Y
PHY2TAGS	—	Y
PHY2VLAN	—	Y
PLUS_ONE	Y	—
PORT_MIRRORING	—	Y
PORTAUD	—	Y
PORTVID	—	Y
PRESENCE_LIST_REQUEST_URI_FORMAT	Y	—
PRESENCE_SERVER	—	Y
PRESENCE_SERVER_IN_USE	—	Y
PROCSTAT	Y	—
PROVIDE_CF_RINGTONE	Y	—
PROVIDE_EDITED_DIALING	Y	—

Table continues...

Name	Supported on 96xx phones	Supported on H175
PROVIDE_EXCHANGE_CALENDAR	Y	—
PROVIDE_EXCHANGE_CONTACTS	Y	—
PROVIDE_KEY_REPEAT_DELAY	Y	—
PROVIDE_LOGOUT	Y	—
PROVIDE_NETWORKINFO_SCREEN	Y	—
PROVIDE_OPTIONS_SCREEN	Y	—
PROVIDE_TRANSFER_TYPE	Y	—
PS_XMPP_SERVER_IN_USE	—	Y
PUSHCAP	Y	—
PUSHPORT	Y	—
QKLOGINSTAT	Y	—
RDS_INITIAL_RETRY_ATTEMPTS	—	Y
RDS_INITIAL_RETRY_ATTEMPTS	—	Y
RDS_INITIAL_RETRY_TIME	—	Y
RDS_MAX_RETRY_TIME	—	Y
RDS_SUBSEQUENT_RETRY_ATTEMPTS	Y	—
RECOVERYREGISTERWAIT	—	Y
REDIRECT_TONE	—	Y
REGISTERWAIT	—	Y
REMOTE_LOG_ENABLED	Y	—
RESET_NEEDED	Y	—
RESOURCE_MEMORY_LIMIT	Y	—
RESTART_COUNTER	Y	—
RINGTONESTYLE	—	Y
RFS_DOWNLOAD_STATUS	Y	—
RFSNAME	Y	—
RFSNAME_IN_USE	Y	—
RINGTONES_UPDATE	Y	—
RTCPFLOW	Y	—
SBMBRIGHTNESS1	Y	—
SBMBRIGHTNESS2	Y	—
SBMBRIGHTNESS3	Y	—
SBMCONTRAST1	Y	—
SBMCONTRAST2	Y	—

Table continues...

Name	Supported on 96xx phones	Supported on H175
SBMCONTRAST3	Y	—
SCREENSAVERON	Y	—
SECURECALL	Y	—
SELECT_RINGING_BRIDGED_APP_ON_OFF_HOOK	Y	—
SELECT_RINGING_CALL_APP_ON_OFF_HOOK	Y	—
SERVER_LINE_APPEARANCE_ID_FORMAT	—	Y
SERVER_LINE_OWNER_DOMAIN_FORMAT	—	Y
SERVER_LINE_OWNER_FORMAT	—	Y
SHOW_BLOCK_CAMERA_INFO_POPUP	—	Y
SIG	Y	—
SIG_IN_USE	Y	—
SIGNAL_P_CONFERECE_SIP_HEADER	—	Y
SIGNALING_ADAPTOR	—	Y
SIMULTANEOUS_REGISTRATIONS	—	Y
SIP_HOLD_UNHOLD_RETRY_DELAY_MSEC	—	Y
SIP_PORT_SECURE	—	Y
SIPCONFERENCECONTINUE	—	Y
SIPPORT	—	Y
SIPPROXYSRVR	Y	—
SIPREGPROXYPOLICY	Y	Y
SIPSIGNAL	Y	—
SKILLSCREENTIME	Y	—
SKINS	Y	—
SLMCAP	Y	—
SLMCLIENT	Y	—
SLMCTRL	Y	—
SLMFSB	Y	—
SLMPERF	Y	—
SLMPORT	Y	—
SLMSRVR	Y	—
SLMSTAT	Y	—
SLMTEST	Y	—
SNMPADD	Y	—
SNMPSTRING	Y	—

Table continues...

Name	Supported on 96xx phones	Supported on H175
SNTP_SYNC_INTERVAL	Y	—
SNTP_SYNC_RANDOMIZATION_INTERVAL	Y	—
SPEAKERSTAT	Y	—
SUBSCRIBELIST	Y	—
SUBSCRIBE_LIST_NON_AVAYA	—	Y
SUBSCRIBE_SECURITY	—	Y
SUPPORT_GIGABIT	Y	—
SYSTEM_LANGUAGE	Y	—
TCP_PORT_LOW	Y	—
TCP_PORT_RANGE	Y	—
TEAM_BUTTON_REDIRECT_INDICATION	Y	—
TEAM_BUTTON_REDIRECT_OVERRIDE	Y	—
TEAM_BUTTON_RING_TYPE	Y	—
TEAM_BUTTON_RING_TYPE_PER_BUTTON	Y	—
TLS_SECURE_RENEG	—	Y
TOGGLENAMENUMBER	Y	—
TPSLIST	Y	—
TRANSFER_UPON_HANGUP	Y	—
UDP_PORT_LOW	Y	—
UDP_PORT_RANGE	Y	—
USE_ALSIP_UA_NATIVE_TRANSPORT_LIBRARY	—	Y
USE_EXCHANGE_CALENDAR	Y	—
USE_EXCHANGE_CONTACTS	Y	—
USE_KEY_REPEAT_DELAY	Y	—
USE_PERSON_ELEMENT_FOR_PRESENCE	Y	—
USE_QUAD_ZEROES_FOR_HOLD	—	Y
USER_HSEQUAL	Y	—
UIDISPLAYTIME	Y	—
VIDEO_CALL_DISPLAY_MODE	—	Y
VIDEO_H264_PROFILE	—	Y
VIDEO_MAX_RX_BANDWIDTH	—	Y
VIDEO_MAX_RX_BANDWIDTH_USER	—	Y
VIDEO_MAX_RX_RESOLUTION	—	Y
VIDEO_MAX_TX_BANDWIDTH	—	Y

Table continues...

Name	Supported on 96xx phones	Supported on H175
VIDEO_MAX_TX_BANDWIDTH_USER	—	Y
VIDEO_MAX_TX_RESOLUTION	—	Y
VIDEO_PACKET_LOSS_PROTECTION	—	Y
VIDEO_PAYLOAD_LENGTH	—	Y
VLANSEP	—	Y
VU_MODE	Y	—
VU_PRIMARY_PHONE	Y	—
VU_TIMER	Y	—
WAIT_FOR_INVITE_RESPONSE_TIMEOUT	—	Y
WAIT_FOR_REGISTRATION_TIMER	—	Y
WAIT_FOR_UNREGISTRATION_TIMER	—	Y
WML_PASSWORD	Y	—
WML_REALM	Y	—
WML_USER_ID	Y	—
WMLEXCEPT	Y	—
WMLHELPSTAT	Y	—
WMLHOME	Y	—
WMLIDLETIME	Y	—
WMLIDLEURI	Y	—
WMLPORT	Y	—
WMLPROXY	Y	—

Index

A

AADS server configuration	32
activate the Settings app in the administrator mode	45
administration methods	32
administrator password	44
application installation	55
CSDK-based application package names	59
setting up CSDK-based applications	58
application installation policy	57
applications	
installation	55
uninstalling pushed applications	56
automatic upgrade	61
Avaya telephony applications	59
Avaya Vantage overview	11

B

black list	57
------------------	--------------------

C

certificates	51
management	50
checklist	
device configuration	43
installation	16
server configuration	28
Collaboration Station	
connecting to the network	26
configure the log settings	63
configure the settings file	38
configuring device	
using DHCP	33
connecting	
wired handset	24
wireless handset	24
connecting the Collaboration Station to the network	26
connectors and controls	12
corrupt firmware	66
corrupt system file	66
CSDK-based applications	
package names	59
CSDK parameters	122

D

debug report	
generating	64
opening	65
device configuration	32

device configuration checklist	43
device settings	
file server	45
device upgrade	60
DHCP	
option 43 codes	34
options configuration	33
setting up a DHCP server	29
site-specific parameters	35
DHCPACK	
parameter configuration	35
DHCP server configuration	29
DHCP settings worksheet	19
DHCP site-specific option number	48
DNS configuration	46
document changes	9

E

emergency numbers	
parameters	103
Ethernet settings	89

F

Failover and survivability	63
features	19
file server	
setting up	30
setting up address	45
file server configuration	29
firmware got corrupted	66

G

Google Play Store	
access rules	57
black and white lists	57

H

handset	
connecting	23 , 24
cradle	23
wireless	24
hardware requirements	
software requirements	16
hardware specifications	19
HTTP proxy settings	47

I		
IEEE 802.1.x settings	91	
InSite Knowledge Base	70	
install applications	55	
CSDK-based application package names	59	
installation checklist	16	
L		
layout	11	
legal notices		
LLDP		
content transmitting in LLDP frames	41	
overview	40	
TLV impact on system parameter values	42	
log settings		
configuring settings	63	
N		
networking		
connecting the Collaboration Station	26	
network parameters	82	
Ethernet settings	89	
general settings	82	
IEEE 802.1.x settings	91	
VLAN settings	89	
non UI related operational parameters		
active phone application	101	
server addresses and ports	92	
server configuration		
parameters	92	
third party applications	101	
O		
optional components	14	
P		
parameters		
Avaya Breeze CSDK	122	
Avaya Vantage Basic parameters	129	
dial plan parameters	103	
emergency numbers	103	
general accounts IDs & passwords	118	
general phone functionality	73	
logging and debugging parameters	111	
network parameters	82	
non UI related operational parameters	100	
parameters for controlling configuration parameter		
download	72	
phone lock	120	
phone specific parameters	73	
phone UI related settings	74	
parameters (continued)		
protocol-specific parameters	103	
security	122	
unsupported configuration parameters	134	
upgrade related parameters	115	
password security policies	50	
physical device layout	11	
ping a device on the network	65	
ports	12	
power outage during upgrade	66	
power sources	26	
PPM	31	
prerequisites	16	
push application on the device		
examples	56	
push applications	55	
R		
reboot	63	
recovery procedure	66	
related documentation	68	
requirements		
hardware	16	
software	16	
reset a device to factory settings	62	
S		
secure installation		
parameters	52	
security	48	
server		
setting up a DHCP server	29	
server configuration	28	
AADS	32	
DHCP	29	
file server	29	
System Manager	31	
server configuration checklist	28	
Session Border Controller		
configuring	30	
Settings app		
administrator mode	45	
settings file	37	
configuring	38	
customizing	38	
worksheet	18	
Settings screen		
AADS configuration	46	
DNS configuration	46	
HTTP proxy and exception	47	
SIP server	47	
SIP server settings	47	
site-specific options		
list of parameters	36	
software specifications	19	

specifications	19
wireless handset	20
support	70
supported accessories	19
System Manager configuration	31
System Manager user profile worksheet	17

T

third party applications	
parameters	101
TLV impact on system parameter values	42
troubleshooting	66

U

uninstall pushed applications	56
upgrade	60
automatic upgrade	61
procedure	60
using System Manager	61
using Update Now option	62
USB parameters	114
user group	46
configuring using settings file	40

V

videos	70
VLAN settings	89

W

white list	57
wired handset	
connecting	24
wireless handset	24
features	21
layout	15
LED indication	22
multifunction button functionality	23
specifications	20
worksheets	
DHCP settings worksheet	19
settings file worksheet	18
System Manager user profile worksheet	17