



Avaya Aura® Device Services Release Notes

Release 10.2.0.1
Issue 1
May 2024

Notice

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

Documentation disclaimer

“Documentation” means information published 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](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 LLC., 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 LLC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

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

License types

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

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “**Unit**” means the unit on which Avaya, at its sole discretion, bases the

pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named User,” means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

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 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](http://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 15 <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>).

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 LLC.

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.

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.

Contents

Change History.....7

Introduction 7

Product compatibility 7

Support Documents.....7

Deployment Considerations.....7

 Upgrade from 10.2.0.0.70 to 10.2.0.1.16.....7

 Software only deployment: Upgrade from 10.2.0.0.70 to 10.2.0.1.16 8

 Additional supported upgrade paths for AADS 10.2.0.1.16 8

Utility Server Application Instructions.....8

 New Virtual IP for Utility Server Services 8

 Firmware Upload Custom File upload Feature 8

 Phone Backup Feature 8

 Utility Server Admin Access 8

 Enable HTTP interface for AADS- Utility Services.....8

What's New in this Release 8

Defect Summary in 10.2.0.1 9

Known issues and workarounds 9

Contact Support Checklist 12

Contact Support Tasks 12

Acronyms 13

Change History

Issue	Date	Description
1	14-May-2024	GA Release of Avaya Aura® Device Services Release 10.2.0.1

Introduction

This document provides late-breaking information to supplement the Avaya Aura® Device Services 10.2 software and documentation.

Product compatibility

For the latest and most accurate compatibility information go to <https://support.avaya.com/CompatibilityMatrix/Index.aspx>

Support Documents

	URL
Avaya Aura Device Services 10.2 Deployment Guide	https://downloads.avaya.com/css/P8/documents/101087711
Avaya Aura Device Services 10.2 Administering Guide	https://downloads.avaya.com/css/P8/documents/101087709

Deployment Considerations

IMPORTANT:

It would be recommended to take a snapshot of existing load before the upgrade.

Rollback to previous AADS version < 10.2.0.1 is not supported

Upgrade from 10.2.0.0.70 to 10.2.0.1.16

- Upgrade SMGR to the latest 8.1/10.1/10.2 GA load if needed
- Upgrade SM(s) to the latest 8.1/10.1/10.2 GA load if needed
- Download AADS 10.2 binary to admin user's home directory
- Set executable permissions to AADS 10.2.0.1.16 binary
 - `chmod 750 aads-10.2.0.1.16.bin`
- Remove inactive versions(if any) using command `app removeinactive`
- Use terminal multiplexer command "tmux" (useful in case if ssh connection drops during install/upgrade)
 1. Start the install/upgrade on a tmux session
 - To start tmux session, run
 - a. `tmux`
 - b. Run install/upgrade as usual
 - c. `app install <absolute path of aads-10.2.0.1.16.bin>`
 - 2. If the ssh terminal hangs or disconnects, login to vCenter VM console
 - a. First list all tmux sessions
 - b. `tmux ls` # output as shown below, the circled integer is session_id that will be used to re-attach in Step 3
 - c. `0: 1 windows (created Wed Feb 15 02:41:37 2023) [189x51]`
 - 3. To reattach to the running tmux session, shown in Step 1 above
 - a. `tmux attach-session -t 0`
 - b. the screen should re-attach to earlier screen created using tmux

Note: If cluster setup, please install "aads-10.2.0.1.16.bin" first on seed node, later repeat this step for all other non-seed nodes

- Once installation/upgrade is done with all nodes, restart AADS services on seed node first. Once services on seed node are up and running, restart aads

Copyright 2018-2024 Avaya LLC All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

services on other nodes in cluster.

Software only deployment: Upgrade from 10.2.0.0.70 to 10.2.0.1.16

- Upgrade SMGR to the latest 8.1/10.1/10.2 GA load if needed
- Upgrade SM(s) to the latest 8.1/10.1/10.2 GA load if needed
- Download AADS 10.2.0.1.16 binary to admin user's home directory
- Set executable permissions to AADS 10.2.0.1.16 binary

```
chmod 750 /home/admin/aads-10.2.0.1.16.bin
```

- Install AADS 10.2.0.1.16 binary

```
app upgrade /home/admin/aads-10.2.0.1.16.bin
```

- **Note:** If cluster setup, please install "aads-10.2.0.1.16.bin" first on seed node, later repeat this step for all other non-seed nodes
- Once installation/upgrade is done with all nodes, restart AADS services on seed node first. Once services on seed node are up and running, restart aads services on other nodes in cluster.

Additional supported upgrade paths for AADS 10.2.0.1.16

Following upgrade paths are also supported for AADS 10.2.0.1.16 upgrade.

1. 10.1.1.0.192 -> SSP6 -> 10.2.0.1.16
2. 10.1.1.1.19 -> SSP6 -> 10.2.0.1.16
3. 10.1.1.2.63 -> SSP6 -> 10.2.0.1.16
4. 10.1.1.3.13 -> SSP6 -> 10.2.0.1.16

Automatic Backup

- AADS 8.1.3 onwards we support automatic backup of existing data and configuration files. Administrators can configure this using AADS admin interface.
- Default backup file password is "RAPtor@WELcomE" . Admin can update it from GUI anytime we want to.

IPv6

- Google Chrome is recommended to login to Admin GUI using Ipv6 address. Mozilla Firefox asks for authentication credentials again for some pages.
- IPv6 is not supported for AWS deployments.
- NTP ,DNS and onboard openLDAP in IPv6 mode only is not supported from AADS 8.0.1

Utility Server Application Instructions

Note: In cluster setup, cluster configuration must be done before utility server configuration

New Virtual IP for Utility Server Services

From 7.1.3.2 release we support port 443 for Utility services.

A new Virtual IP is needed, and would be adding during installation and upgrade process.

Firmware Upload Custom File upload Feature

In clustered environment, Utility Server admin operations like uploading firmware and custom upload files (images, ringtones, Certificates etc) should be done in all nodes using the admin interface of the node in context

Phone Backup Feature

In clustered environment, Phone Backup Feature works only when seed node (first node) is up and running.

Utility Server Admin Access

In clustered or stand alone setups, US Admin ui is accessible with this URL https://<AADS_node_IP_Address>:8543/admin.html Note that admin operations , should be performed on each node in a clustered environment.

Enable HTTP interface for AADS- Utility Services

After upgrading to 10.2.0.1.16, to enable HTTP interface for AADS Utility Server, please run the script
`/opt/Avaya/DeviceServices/10.2.0.1.16/CAS/10.2.0.1.16/misc`

```
sudo ./us-http-port.sh --enable
```

What's New in this Release

The following table lists the enhancements in Avaya Aura® Device Services 10.2.0.1

AADS 10.2.0.1 Release Content	
JIRA	Description
ACS-29576	Support for AD 2022
ACS-29554	Upgrade cassandra to 4.1.3
ACS-29545	Upgrade apache tomcat to 9.0.71

Defect Summary in 10.2.0.1

Ticket ID	Summary	Affects Version/s	Fix Version/s
ACS-29727	Keycloak service not started after upgrade	10.2.0.0	10.2.0.1
ACS-29639	Keycloak Postgress database migration failed	10.2.0.0	10.2.0.1
ACS-29584	Not able to login keycloak admin GUI after upgrade when select oauth option yes during upgarde	10.2.0.0	10.2.0.1
ACS-29553	Workplace client doesn't receive BSM IP in case main SM is unreachable	8.1.5.x/10.1.x/10.2	10.2.0.1
ACS-29608	Auto config does not work when SMGR user has 2 communication profile	10.2.0.0	10.2.0.1

Known issues and workarounds

Key	Summary	Affects Version/s	Release Note
ACS-29628	PEA 1-A4ESQ41 Keycloak page is not opening after upgrading to AADS 10.2. The customer is using 3rd party certificates SR Description: AADS key clock page not working post upgrade 10.2	10.2	Workaround: • Login to AADS server with administrative user • Switch to "root" user • Change "--hostname-admin" from the uppercase to lowercase in "/opt/Avaya/DeviceServices/10.2.0.1.16/CAS/10.2.0.1.16/service.d/keycloak.start.sh" • svc keycloak restart • In case of cluster, repeat above steps for all nodes
ACS-29487	keepalived-config.properties and aads-rules.nft files updations doesn't get updated as part of GUI change when switching to LB	10.1	Workaround: Update AADS_NODE_IP in /etc/nftables/aads-rules.nft manually if switched from internal LB to external LB, o.w. not required ip daddr <AADS_NODE_IP> tcp dport 443 counter packets 0 bytes 0 redirect to :8443
ACS-29461	Not able to login keycloak admin GUI after rollback	10.2	Workaround: Use Vmware snapshot feature before upgrade to 10.2

ACS-18780	Languages in Assign License and LDAP Group Auto Assign pages are full of special characters	8.1.3	Workaround in case of language characters are corrupted in 'Assign licesne' page after migration or fresh installation. Run below clitool command with the options provided. sudo ./clitool-acs.sh languageORTimeZoneUpdate <lang properties path> true true <lang properties path> if the path of file having extension as .properties and the entries given below: English=en-US Deutsch - German=de-DE español - Spanish=es-LA français (Canada) - French (Canada)=fr-CA français (France) - French (France)=fr-FR italiano - Italian=it-IT 日本語 - Japanese=ja 한국어 - Korean=ko-KR português - Portuguese (Brazil)=pt-BR русский - Russian=ru 中文（简体） - Chinese (Simplified)=zh-CN 中文（香港） - Chinese (Hong Kong) =zh-HK
ACS-15770	missing the data encryption instruction when deploying on SDM integrated with SMGR 8.0.1	8.0.1	Please check with SDM version 8.1 and onwards to get the complete display of data encryption parameters during OVA deployment using SDM.
ACS-11573	CEC-030 178428-070 P1 Personal Data Minimization D Retention - Log Management- Anonymization		When upgrading from 8.0 to 8.0.1 AADS , before executing force ldap sync , run clearPhoneNumberLastSync.sh from misc directory of installation. To makes sure that the all the data is synced again Run the following steps only on seed node, 1. Login to aads seed node 2 run command:- cdto misc 3 run command : - sudo ./clearPhoneNumberLastSync.sh
ACS-11474	[AADS 8.0.SP1 FIPS- STIG] Unable to login US admin or AADS Admin GUI after applying STIG	8.0.0.1	Cannot log into admin GUI using Linux credentials . Once STIG is enabled this is the expected behaviour. Solution - Login in using LDAP credentials belonging to the AADS Administrator Role. - If the Administrator Role is not properly configured and admin cannot login using LDAP credentials, then configure it by running "app configure" from the Linux command line and navigating to "LDAP Configuration". From there configure the "Administrator Role" as described in the "LDAP configuration" section of the Deploying the Avaya Aura® Device Services document.
ACS-11122	Import IDP.xml: Some special chars incorrect mapping between bluetool and admin GUI	8.0.1	Workaround is to continue using the keycloak admin UI on browser to enter any complicated Admin/User roles.
ACS-10607	failed to configure secure onboard OpenLDAP	8	Problem: if secure openldap connection fails due to "java.security.cert.CertificateException: No subject alternative DNS name matching localhost.localdomain found" Solution: Re generate certificates using "app configure" 1. Run command "app configure" 2. Select "Front-end host, System Manager and Certificate Configuration" 3. Provide "System Manager Enrollment Password" and "Keystore password" 4. Select "Apply" and continue further to restart AADS service
ACS-10583	Adding keycloak user / group DN with space causes installer to think field is blank	8	Issue : While configuring keycloak When prompted to enter the DN for the admin or user role, enter a DN that contains special characters (like / \, and space etc).The installer does not proceed and displays an error "The value cannot be blank" Solution : Can remove all special characters and then log into the keycloak admin UI afterwards to re-enter the special characters

ACS-10537	[IPv6] Admin UI: Authentication Required on Dynamic Configuration page	8	Google Chrome is recommended to login to Admin GUI using Ipv6 address. Mozilla firefox asks for authentication credentials again for some pages.
ACS-7269	Dynamic config group search fails if any LDAP is down in multi-LDAP setup	7.1.5	Description In multi-LDAP setup, when searching for groups in Dynamic Configuration, if one of the LDAP is down, the group search stops and fails even if the LDAP containing the group is up. In particular, if the onboard openLDAP is enabled but slapd is down, then ALL remaining LDAP will never be searched. Steps to reproduce Enable the onboard OpenLDAP during installation of AADS 7.1.5.0.78 Add two or more LDAPS to AADS Shutdown the slapd process on AADS (onboard OpenLDAP) Go to the Dynamic Configuration screen, publish screen Select group and start typing in a group you know exists in one of the LDAP Result: The search fails to find any groups at all. The search seems to fail on the first LDAP that is down (onboard OpenLDAP) and then skips searching all the remaining LDAP. Workarounds: Need to ensure all the LDAP managed on AADS are up and do not return any exceptions while being searched by the Dynamic Configuration service.
ACS-6184	1543 port shouldn't work in Utility Server on 7.1.3.2.xx load	7.1.3.2	Issue : In addition to 443 port , 1543 port remains open for Utility Services .
ACS-5885	Child Domain users fail to authenticate when Multiple Auth Domains configured	7.1.3.1	Prior to adding a second domain, if the base context being used is high in the directory tree (e.g. a top-level domain), and there are subdomains: - The high-level base context DN must be replaced with multiple base context DNs - one for each subdomain E.g. If the base context DN is: DC=avaya,DC=com and there are users in subdomains such as DC=global,DC=avaya,DC=com, DC=west,DC=avaya,DC=com and DC=east,DC=avaya,DC=com.

			Then the single base context DN DC=avaya,DC=com must be replaced with 3 base context DNs: DC=global,DC=avaya,DC=com DC=west,DC=avaya,DC=com DC=east,DC=avaya,DC=com Otherwise, a user in one of the subdomains that was previously able to authenticate prior to adding the additional domain will no longer be able to authenticate. The reason is that once multiple domains are introduced, the authenticator tries to find the correct directory to send an authentication request to based on an exact match of the user's domain with the configured base context DNs. This will be fixed in a later release such that the code will recognize that subdomains are part of the higher-level domain. Note: The administration UI prevents adding subdomain base contexts. The above procedure must be used if multiple base contexts are subdomains.
ACS-5735	Inclusion the T attribute in the Subject CN of the CA in SMGR CA , causes AADS installation to fail	7.1.3	Issue : Inclusion the T attribute in the Subject CN of the CA in SMGR CA , causes AADS installation to fail Solution: Modify the CA to remove the T attribute. All previously generated certificates using this CA will need to be regenerated.
ACS-24203	Test button on Client Id Mapping page to test oauth flow fails with an exception	8.1.5	Solution: Workplace client can be used to test the oauth login.
ACS-24520	Ldap partition Quick Search feature is not working after upgrading from 8.1.4.0	8.1.5	Issue : Ldap partition Quick search (Quick search within same OU) is not working after upgrade from 8.1.4.0 to 8.1.5.0 Solution: Run the following steps only on seed node, 1. Login to aads seed node 2. run command:- cdto misc 3. run command : - sudo ./clearPhoneNumberLastSync.sh 4. Login to AADS Admin UI → Navigate to Server Connections page → Force Ldap sync Note: Those steps are not required if the system is upgraded from 8.1.4.1 to 8.1.5.0
ACS-25464	system layer upgrade from 4.0.0.0.3 to 4.0.0.0.4 got stuck at 240 seconds when stating service. httpd, keycloak and symmetricds are not come up	10.1	Issue: All AADS service are not up and running on reboot of system after applying system layer patch 4.0.0.0.4 Solution: If AADS services are not within 5 minutes of system reboot, start AADS services manually using "svc aads start" command.

Contact Support Checklist

If you are having trouble with an Avaya Workplace Client, you should:

1. Set log level to debug.
2. Retry the action. Carefully follow the instructions in written or online documentation.
3. Check the documentation that came with your hardware for maintenance or hardware-related problems.
4. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.

If you continue to have a problem, contact Avaya Technical Support:

1. Log in to the Avaya Technical Support Web site <https://support.avaya.com>.
2. Contact Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site.

Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information, see the Escalation Contacts listings on the Avaya Web site.

Contact Support Tasks

Copyright 2018-2024 Avaya LLC All rights reserved.
Use pursuant to the terms of your signed agreement or Avaya policy.

You may be asked to email one or more files to Technical Support for analysis of your application and its environment.

Acronyms

Acronym	Definition
Acronym	Definition
3PCC	Third Party Call Control
AAC	Avaya Aura® Conferencing
AADS	Avaya Aura® Device Services
AAWG	Avaya Aura® Web Gateway
AEMO	Avaya Equinox® Meetings Online
AMM	Avaya Multimedia Messaging
ASBCE	Avaya Session Border Controller for Enterprise
BLA	Bridged Line Appearance
CM	Avaya Aura® Communication Manager
FP	Feature Pack
MDA	Multiple Device Access
MSS	Multi-Stream Switching
OTT	Over The Top
POM	Presentation Only Mode
PS	Avaya Aura® Presence Services
SM	Avaya Aura® Session Manager
SMGR	Avaya Aura® System Manager
SP	Service Pack
SRTP	Secure Real-Time Transport Protocol
TOM	Top of Mind
TLS	Transport Layer Security
UC	Unified Communication