Release Notes AADS - 10.1.1.0

Avaya Aura® Device Services 10.1.1.0.192 Release Notes

Introduction

This document provides late-breaking information to supplement the Avaya Aura® Device Services 10.1.1.0 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 10.1.1.0 Deployment Guide	https://downloads.avaya.com/css/P8/documents/101079251
Avaya Aura Device Services 10.1.1.0 Administering Guide	https://downloads.avaya.com/css/P8/documents/101079249

Deployment Considerations

The old 10.1 GA OVA contains the Avaya Signing certificate that is going to expire on Feb 20, 2023.

Therefore, to address the Avaya signing certificate expiry, the new 10.1 GA OVAs are renewed and re-signed with the latest Avaya signed certificates.

Refer PSN006175 for details.

Note:

- **AADS 10.X does not support ESXi 6.5.**

IMPORTANT:

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

Fresh Install 10.1.1.0.192

- Upgrade SMGR to the latest 8.1/10.1.x load if needed
- Upgrade SM(s) to the latest 8.1/10.1.x load if needed
- Deploy AADS 10.1.1.0.192 OVA
- Run AADS 10.1.1.0.192 binary

```
app install
```

Upgrade from 10.1 GA Build 120 to 10.1.1.0.192

- Upgrade SMGR to the latest 8.1/10.1 GA load if needed
- Upgrade SM(s) to the latest 8.1/10.1 GA load if needed
- Check version of the system layer using command: "sys versions" . No need to upgrade the system layer if it is already 4.0.0.0.7
- Update to a new system layer 4.0.0.0.7
  Note:
  - if cluster setup, please update system layer on all nodes before next step
  - In case if AADS services are not up and running after applying system layer patch 4.0.0.0.7, please start it manually
    - svc aads start
- Update to new SSP2
  - Download SSP2 to admin user's home directory.
  - `svc aads stop`
  - `av-update-os AV-AADS10.1-RHEL8.4-SSP-002-04.tar.bz2`
  - SSP2 installation reboots the server at the end. After reboot, verify Security Service Pack 2 version
    - *av-version*
    - It shows the output as below

      OS_VERSION: Red Hat Enterprise Linux release 8.4 (Ootpa)
      AV_SSP_VERSION: 002
      AV_BUILD_NUMBER: 04

  - `svc aads start`
- Download AADS 10.1.1.0.192 binary to admin user's home directory
- Set executable permissions to AADS 10.1.1.0.192 binary

  ```
  chmod 750 /home/admin/aads-10.1.1.0.192.bin
  ```

- Install AADS 10.1.1.0.192 binary

  ```
  app upgrade /home/admin/aads-10.1.1.0.192.bin
  ```

  Note: If cluster setup, please install "aads-10.1.1.0.192.bin" first on seed node, later repeat this step for backup node
- Once installation/upgrade is done with all nodes, start AADS services

Upgrade from 10.1.0.1.46 (10.1 SP1) to 10.1.1.0.192

- Upgrade SMGR to the latest 8.1/10.1 GA load if needed
- Upgrade SM(s) to the latest 8.1/10.1 GA load if needed
- Check version of the system layer using command: "sys versions" . No need to upgrade the system layer if it is already 4.0.0.0.7
- Update to a new system layer 4.0.0.0.7
  Note:
  - if cluster setup, please update system layer on all nodes before next step
  - In case if AADS services are not up and running after applying system layer patch 4.0.0.0.7, please start it manually
    - svc aads start
- Update to new SSP2
  - Download SSP2 to admin user's home directory.
  - `svc aads stop`
  - `av-update-os AV-AADS10.1-RHEL8.4-SSP-002-04.tar.bz2`
  - SSP2 installation reboots the server at the end. After reboot, verify Security Service Pack 2 version
    - *av-version*
    - It shows the output as below

      OS_VERSION: Red Hat Enterprise Linux release 8.4 (Ootpa)
      AV_SSP_VERSION: 002
      AV_BUILD_NUMBER: 04

  - `svc aads start`
- Download AADS 10.1.1.0.192 binary to admin user's home directory
- Set executable permissions to AADS 10.1.1.0.192 binary

  ```
  chmod 750 /home/admin/aads-10.1.1.0.192.bin
  ```

- Install AADS 10.1.1.0.192 binary

```
app upgrade /home/admin/aads-10.1.1.0.192.bin
```

Note: If cluster setup, please install "aads-10.1.1.0.192.bin" first on seed node, later repeat this step for backup node

- Once installation/upgrade is done with all nodes, start AADS services

Software only deployment: Fresh Install 10.1.1.0.192)

- Upgrade SMGR to the latest 8.1/10.1.x GA load if needed
- Upgrade SM(s) to the latest 8.1/10.1.x GA load if needed
- Copy AADS 10.1.1.0.192 swonly artifact to server
- Login with "root" user and Apply swonly system layer first

```
tar -xzf aads-swonly-10.1.1.0.192.tgz
cd aads-swonly-10.1.1.0.192
tar -xzf ucapp-swonly-system-2.0.0.0.12
cd ucapp-swonly-system-2.0.0.0.12
./swOnlyUpdate.sh --install
```

- Install AADS 10.1.1.0.192 binary

```
app install <absolute path of aads-10.1.1.0.192.bin>
```

Software only deployment: Upgrade from 10.1 GA Build 120 to 10.1.1.0.192

- Upgrade SMGR to the latest 8.1/10.1 GA load if needed
- Upgrade SM(s) to the latest 8.1/10.1 GA load if needed
- Download AADS 10.1.1.0.192 binary to admin user's home directory
- If Azure instance, please apply the software-only system layer patch first to update the system layer version to 2.0.0.0.12
    - Login as "root" and go to "ucapp-swonly-system-2.0.0.0.12" directory (extracted from software-only artifact aads-swonly-10.1.1.0.192.tgz)
    - Apply the patch using following command

```
./swOnlyUpdate.sh --patch
```

- Set executable permissions to AADS 10.1.1.0.192 binary

```
chmod 750 /home/admin/aads-10.1.1.0.192.bin
```

- Install AADS 10.1.1.0.192 binary

```
app upgrade /home/admin/aads-10.1.1.0.192.bin
```

Note: If cluster setup, please install "aads-10.1.1.0.192.bin" first on seed node, later repeat this step for backup node

- Once installation/upgrade is done with all nodes, start AADS services

Software only deployment: Upgrade from 10.1.0.1.46 (10.1 SP1) to 10.1.1.0.192

- Upgrade SMGR to the latest 8.1/10.1 GA load if needed
- Upgrade SM(s) to the latest 8.1/10.1 GA load if needed
- Download AADS 10.1.1.0.192 binary to admin user's home directory
- If Azure instance, please apply the software-only system layer patch first to update the system layer version to 2.0.0.0.12
    - Login as "root" and go to "ucapp-swonly-system-2.0.0.0.12" directory (extracted from software-only artifact aads-swonly-10.1.1.0.192.tgz)
    - Apply the patch using following command

```
./swOnlyUpdate.sh --patch
```

    - Verify system layer version using "sys versions" command, after applying patch it should be "2.0.0.0.12"
- Set executable permissions to AADS 10.1.1.0.192 binary

```
chmod 750 /home/admin/aads-10.1.1.0.192.bin
```

- Install AADS 10.1.1.0.192 binary

```
app upgrade /home/admin/aads-10.1.1.0.192.bin
```

Note: If cluster setup, please install "aads-10.1.1.0.192.bin" first on seed node, later repeat this step for backup node

- Once installation/upgrade is done with all nodes, start AADS services

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 10.1.1.0.192 or installing fresh 10.1.1.0.192 to enable HTTP interface for AADS Utility Server, please run the script /opt/Avaya /DeviceServices/10.1.1.0.192/CAS/10.1.1.0.192/misc

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

What's New in this Release

The following table lists the enhancements in Avaya Aura® Device Services 10.1.1.0

AADS 10.1.1.0 Release Content	
JIRA	**Description**
ACS-26237	Decoupling AADS-Aura
ACS-26727	AADS Performance Benchmarking and Modelling
ACS-26725	Technical Debt- 10.1.1.0
ACS-26982	AADS Core Components Upgrade
ACS-27535	Validate AADS performance after enabling Nested Groups Support on AADS for Dynamic config
ACS-27670	AADS 10.1.1.0 CECs

Fixed Issues in 10.1.1.0

Ticket ID	Summary	Affects Version /s	Fix Version /s
ACS-28408	IX Meeting 9.1.14 CD6 - P2S2- Unable to login Portal after upgrading AADS from 10.1.0.0.112 to 10.1.1.0.148	10.1.0.0	10.1.1.0
ACS-28343	AADS 10.1.0.0 SSH CBC ciphers are allowed despite SSH config file	10.1.0.0	10.1.1.0
ACS-28141	Not possible to change the Settings in AADS for Field "SCREEN_POP_LIST"	8.1.5.0	10.1.1.0
ACS-28029	Allow port 8443 to be used for reverse proxy	10.1.0.1	10.1.1.0
ACS-28024	[SWonly] The backup fails if system has java version "1.8.0.332.b09-1.el8_5" OR later	10.1.0.0	10.1.1.0
ACS-27955	[AADS SSP2] AADS not inactive SSH session timeout after 10 minute	10.1.0.1	10.1.1.0
ACS-27924	Uninstallation of AADS removes "/opt/avaya" directory	10.1.0.0	10.1.1.0
ACS-27921	Keycloak Server-Side Request Forgery vulnerability	8.1.5.0	10.1.1.0
ACS-27898	The AADS backup fails after applying SSP 2	10.1.0.0	10.1.1.0
ACS-27881	Alarms fail on aads when it is added to an existing TLSv1.3 enabled cluster	10.1.0.0	10.1.1.0
ACS-27672	Identity certificate generation via SMGR fails	10.1.0.1	10.1.1.0
ACS-27649	Utility Server Phone backup is failing	10.1.0.0	10.1.1.0
ACS-27644	AADS spirit agent is not seen on SMGR due to ciphers support on AADS	8.1.5.0	10.1.1.0
ACS-27500	AADS UI Unable to configure PHNOL filed with #9 value. Error “This is an invalid value for PHNOL.	8.1.4.0	10.1.1.0
ACS-27441	Update contact with new default phone number (isPrimary) doesn't work	8.1.5.0	10.1.1.0
ACS-27410	Alpha Green AADS : Server hang with no ssh and webadmin, user login failed.	10.1.0.1	10.1.1.0
ACS-27260	Change of TLS from 1.2 to 1.3 now can't repair AADS Node from SMGR due to DRS has failed SM and AADS are not talking	10.1.0.1	10.1.1.0
ACS-27110	SMGR is not being searched while performing Unified / Enhanced Search with Aura Enabled	10.1.9	10.1.1.0
ACS-27099	Correct message and note for "Aura Support" option in bluetool	10.1.9	10.1.1.0
ACS-27064	CPU utilization is 100% (users with specific phone numberes) on both AADS while searching by clients	8.1.5.0	10.1.1.0
ACS-27036	NULL values in Alarms 0184 0185 [System Throughput: null][CPU Percentage: null]	8.1.5.0, 10.1.0.0	10.1.1.0
ACS-27016	GDPR incorrect file numbering	8.1.4.1	10.1.1.0
ACS-27014	AADS utility admin page returns SMGR cert when using 3rd party CA certs	8.1.5.0	10.1.1.0
ACS-26950	Character $ in keystore password breaks secure LDAP connection	8.1.4.0	10.1.1.0
ACS-26799	Test connection fails for onboard openldap configuration during interactive installation	10.1.0.0	10.1.1.0
ACS-26772	Getting error java.lang.IllegalArgumentException during running run UserDiagnostics tool	10.1.0.1	10.1.1.0
ACS-26209	An error "Corporate directory not available" occurred for users whose emails contain special characters	8.1.4.1	10.1.1.0
ACS-28314	[10.1.1.0] AADS clusters deployed on Azure unable to access to Utility Server Virtual IP/FQDN	10.1.0.0	10.1.1.0

Known issues and workarounds

Key	Summary	Affects Version/s	Release Note
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 extention 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 - Japanese=ja - Korean=ko-KR português - Portuguese (Brazil)=pt-BR - Russian=ru - Chinese (Simplified)=zh-CN - 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 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-1	Adding keycloak user / group DN with space causes installer to think field is blank	8	Issue : While confugring 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"

0583			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-72769	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-61184	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-58885	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-57735	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 runnning 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 Equinox 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

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

Acronyms

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