AVAYA

Avaya Breeze® platform Release Notes

Release 3.8 GA
Issue 3
October 2020

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: http://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, HTTP://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, HTTP://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 Section M(i)1 or 2 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.

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 http://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products," or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Contact Avaya Support

See the Avaya Support website: http://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: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

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.

Table of Contents

Change history

Issue	Date	Description
1	Sep 4, 2020	GA Release of Avaya Breeze® platform 3.8.
2	Sep 8, 2020	Updated section for new alarms.
3	Oct 23, 2020	Updated Zang SMS Connector version.

Issues fixed in this release

1	**Problem Resolved:**	1. Initially, Breeze 3.8 is registered successfully with SMGR Geo-R pair (Primary & Secondary) 2. Later on due to some reason Primary SMGR is converted to Standalone SMGR 3. Breeze switched to Standalone SMGR 4. Breeze is not be able to sync (DRS replication) with standalone SMGR. As a result Breeze is not managed by SMGR.
	Reference:	Zephyr-69240
	Keywords:	DRS Synchronization , Geo-R, Failover
2	**Problem Resolved:**	CEnetSetup does not update http_proxy/https_proxy setting in /etc/profile.d/proxy.sh; outbound proxy will not work.
	Reference:	Zephyr-69199
	Keywords:	Outbound proxy, CEnetSetup, installation
3	**Problem Resolved:**	Authentication and Authorization stored cookies prevents user logout action.
	Reference:	Zephyr-69025
	Keywords:	Authorization, logout
4	**Problem Resolved:**	Breeze not processing “Decline” correctly when attempting to add an Equinox Attendant that is not currently accessible. .
	Reference:	Zephyr-68980
	Keywords:	Equinox Attendant, SIP, addParticipant
5	**Problem Resolved:**	Oceana solution upgrade script fails with large ISO download due to connection timeout of ssh session
	Reference:	Zephyr-68933
	Keywords:	upgradeSolution, Oceana
6	**Problem Resolved:**	Oceana solution upgrade script not cleaning up after successful upgrade.
	Reference:	Zephyr-68742
	Keywords:	upgradeSolution, Oceana
7	**Problem Resolved:**	Called party 1 not dropped when Calling party hangs up, downstream forking
	Reference:	Zephyr-68729
	Keywords:	Downstream forking, SIP, Callable, Call Intercept
8	**Problem Resolved:**	upgradeSolution script failure caused by insufficient disk space in /var
	Reference:	Zephyr-68303
	Keywords:	upgradeSolution, Oceana

Known issues and workarounds

1.	**Problem:**	If a Session Manager 8.1 customer administers Communication Manager Load

		Balancing with an Avaya Breeze® platform 3.x in their configuration, DRS stops working for the Breeze node.
	Workaround:	Avaya Breeze® platform 3.7 or later is required if the “CM Load Balancing” feature in Session Manager 8.1 is enabled. Failure to ensure this will result in the Avaya Breeze® platform node becoming unusable.
	Reference:	Zephyr-67643
	Keywords:	Session Manager-Breeze interaction, CM load Balancing
	Keywords:	Update Port numbers
2.	**Problem:**	Additional procedures are required to upgrade Avaya Breeze® platform in a Dual System Manager configuration.
	Workaround:	For assistance in upgrading Avaya Breeze® platform in a Dual System Manager configuration, contact Avaya Support.
	Keywords:	Dual System Manager
3.	**Problem:**	OPTIONs pings failed from WAS toward ASSET after upgrade. Any SIP operation with outbound OOD (INVITE and REFER) that are going toward Session Manager fail.
	Workaround:	Restart WebSphere by executing “restart WebSphere”.
	Reference:	Zephyr-58959
	Keywords:	WebSphere, SIP, MakeCall
4.	**Problem:**	Demo Certificates not supported with CRL.
	Workaround:	Avaya strongly discourages the use of the deprecated Demo Certificates. If for some reason these are required, they will not work with the Certificate Revocation List (CRL) functionality, and so CRL checking should be disabled.
	Reference:	Zephyr-58182
	Keywords:	CRL, Demo Certificates
5.	**Problem:**	While trying to login to Kibana UI with username and password using the Cluster FQDN/IP, login fails with javascript error.
	Workaround:	Two workarounds can be tried: • Use the Avaya Breeze® platform asset FQDN/IP instead of the cluster FQDN/IP. • Reinstall the CentralizedLoggingService Snap-in.
	Reference:	Zephyr-65401
	Keywords:	Centralized logging, Kibana
6.	**Problem:**	Cluster DB not reachable.
	Workaround:	This could happen only when the cluster DB process starts before eth0 interface is up and is a race condition. Reboot the node (or cluster if required by your application) and if the issue does not resolve, contact Avaya support.
	Reference:	ZEPHYR-67579
	Keywords:	Cluster DB, Cluster DB maintenance test fails
7.	**Problem:**	WARN messages cause flooding the asm.log when running traffic flow using HelloWorld snap-in. For each call you may receive multiple messages.
	Workaround:	Contact Avaya support if the rate of errors is too high or you notice display update issues.

	Reference:	ZEPHYR-68286
	Keywords:	Traffic runs, Logs
8.	**Problem:**	Lambda expressions don't work well with Breeze 3.7 and beyond
	Workaround:	No workaround. Don't use Lambda expressions and use anonymous class equivalents instead.
	Reference:	Zephyr-68025
	Keywords:	Java 8, Lambda Expressions, CallListener not initialized
9.	**Problem:**	Installation status shows installing for a snap-in that accesses Cluster DB not using Hibernate as the JDBC Provider.
	Workaround:	Use hibernate in the snap-in code.
	Reference:	Zephyr-68630
	Keywords:	Installation, ClusterDB
10	**Problem:**	Avaya Real Time Speech not supported in Breeze 3.7 and beyond
	Workaround:	The Avaya Real Time Speech (RTS) Snap-in went end of sale July 31, 2018 and is no longer supported in Avaya Breeze 3.7. The Avaya Breeze 3.7 and 3.8 Javadoc has marked the speech search functionality as deprecated. Refer to the RTS end of sale notice for additional details. https://support.avaya.com/css/P8/documents/101051723
	Reference:	Zephyr-68367
	Keywords:	Real Time Speech
11	**Problem:**	"dasrvstart status all" command shows TPS services being restarted each 10 seconds by Systemd. Manual start of the service from CLI is OK. The Systemd unit file manual "type" defaults to "simple." Since all TPS applications are using forking where a parent process exists, Systemid believes the service is dead and tries to restart it.
	Workaround:	Add "Type=forking" to Systemd unit files.
	Reference:	Zephyr-68682
	Keywords:	Systemd, TPS services
12	**Problem:**	ADA 8.1.1 (or earlier ADA release) will not work with Breeze 3.7 and beyond
	Workaround:	Revert Breeze to Breeze 3.6 Or Install field version of ADA 8.1.1 as described in Avaya KB Solution: SOLN348058
	Reference:	Zephyr-68688
	Keywords:	ADA
13	**Problem:**	HTTP Proxy exclusion list cannot be configured during Breeze OVA deployment
	Workaround:	Run CEnetSetup and select 'y' for "Would you like to configure an HTTP proxy?". The default exclusion list will be local subnet CIDR and network domain.
	Reference:	Zephyr-68720
	Keywords:	Installation

14	**Problem:**	CEnetSetup will not allow proxy hostname with hyphen not supported
	Workaround:	None (requires file modification of proxy hostname validation committed to 3.8.0.1)
	Reference:	Zephyr-68752
	Keywords:	Installation, Outbound Proxy
15	**Problem:**	Element Manager installation wrapper does not check for available/free disk space before starting installation.
	Workaround:	Log in to System Manager and run cd /swlibrary command to go to the software directory library. Run df -h /swlibrary command to ensure adequate space is available. Approximately 600 MB of space is need for the installation.
	Reference:	Zephyr-69194
	Keywords:	Element Manager, Installation
16	**Problem:**	Unable to uninstall older CallEventControl service using Service Management page after newer version is installed on cluster.
	Workaround:	Uninstall older service version using Cluster Administration Editor page.
	Reference:	Zephyr-69234
	Keywords:	Uninstall Service
17	**Problem:**	In Geo redundant setup – if the primary SMGR is down and secondary SMGR is active – a freshly deployed Breeze OVA is unable to establish trust with Secondary SMGR –
	Workaround:	Do not install Breeze ova when Primary SMGR is down. Wait until SMGR primary is up then only install Breeze
	Reference:	ZEPHYR-52616 Geo redundancy - OVA deployment unsuccessful during rainyday
	Keywords:	Geo, Secondary Active, Primary Down, Breeze installation fails
18	**Problem:**	While creating JDBC data source, the input text field URL does not allow '_' character in it. It will fail to create data source by showing error.
	Workaround:	Do not use '_' character in URL input text field.
	Reference:	Zephyr-68981
	Keywords:	JBDC data source
19	**Problem:**	Intercepted calls utilizing geo-redundant AAMS clusters fail to set up and are responded to by Breeze with "400 Bad Request". If Breeze logging is enabled, the following signature will be seen in asm.log. <result response="430"> <description>Object does not exist</description> </result>
	Workaround:	Set the Breeze location to be the same as the co-located AAMS cluster
	Reference:	Zephyr-69407

	Keywords:	Call Scenarios, Geo Redundant AMS
20	**Problem:**	When the Reverse Proxy URL field is populated the internal FQDN is redirected to the external FQDN for Auth
	Workaround:	Contact Avaya for a patch.
	Reference:	Zephyr-69433
	Keywords:	Authorization, Reverse Proxy

Avaya Breeze® platform 3.8 GA load components

Component	Version
Avaya Breeze® platform OVA, ISO, AWS and KVM	3.8.0.0.380018
Avaya Breeze® platform Patch	Check the Avaya support site (support.avaya.com) for the latest recommended patch for 3.8.x
System Manager	Latest SMGR 8.0.1.2 GA version + latest SMGR Hotfix Latest SMGR 8.1.2 GA version + latest SMGR Hotfix Latest SMGR 8.1.3 GA version + latest SMGR Hotfix
Avaya Breeze® 3.8.0.0 Element Manager Package (for use with System Manager 8.0.1.2 and System Manager 8.1.2)	3.8.0.0.380019
Avaya Aura Media Server	8.0.2.127 (Avaya Aura® 8.0.1.2 or 8.1.2) 8.0.2.138 (Avaya Aura® 8.1.3)
SDK	3.8.0.0.380018
WebRTC	3.8.0.0.380018
Avaya WebRTC SDK	3.8.0.0.380018
Authorization	3.8.0.0.380019
External Authorization Client SDK	3.8.0.0.380018
Reliable Event Streaming Adapter	3.8.0.0.380018
Centralized Logging (Used with Oceana)	3.8.0.0.380018
Zang Call Connector	3.8.0.0.380018
Zang SMS Connector	3.8.0.0.1020028

System Manager interoperability

Avaya Aura® System Manager release 8.0.1.2, 8.1.2 or 8.1.3 with the latest SMGR HotFix is supported with the Avaya Breeze® platform 3.8 GA load. See Deploying Avaya Breeze® platform; https://downloads.avaya.com/css/P8/documents/101070661 (chapter 4 *Running the upgradeSolution script for System Manager Release 8.0.1.2 or 8.1.2***)** for more information.

Note: System Manager may release additional Integrated Patches, Hot Fixes etc. that may need to be applied additionally on this GA version.

Avaya Breeze® platform can be deployed with System Manager:

- Release 8.0.1.2 by installing the Avaya Breeze® platform 3.8 Element Manager using the new
- upgradeSolution utility provided in the latest hot fix release of System Manager.
- Release 8.1.2 by installing the Avaya Breeze® platform 3.8 Element Manager using the new
- upgradeSolution utility provided in the latest hot fix release of System Manager.
- Release 8.1.3 with the latest hotfix, which already contains the Avaya Breeze® platform 3.8 Element Manager.

If you are running System Manager Release 8.0.x, you must update your system to Release 8.0.1.2 with the latest published hot fix from https://support.avaya.com. If you are running System Manager Release 8.1.x, you must update your system to Release 8.1.2 or 8.1.3 with the latest published hot fix from https://support.avaya.com. If you are running an earlier version of System Manager, you must update to System Manager 8.1.3.

Deployment of Avaya Breeze® platform Release 3.8 with System Manager Release 8.0.1.2 or 8.1.2 allows you to avoid a full System Manager upgrade. Instead, this deployment requires that you run a special script to install the Avaya Breeze® platform 3.8 Element Manager with the older System Manager.

Important:

When you have applied the Avaya Breeze® platform Release 3.8 Element Manager to System Manager Release 8.0.1.2 or 8.1.2, subsequent integrated patches and hot fixes will leave the 3.8 Element Manager intact and no further action is required to work with Avaya Breeze® platform 3.8.

Caution:

When you have applied the Avaya Breeze® platform Release 3.8 Element Manager to System Manager Release 8.0.1.2, if in the future the System Manager is migrated to 8.1.2 with the latest hot fix, you must reapply the Release 3.8 Element Manager by running the upgradeSolution utility script. The migration will retain all Avaya Breeze® platform Release 3.8 configuration data.

Session Manager interoperability

Avaya Breeze® platform 3.3 or later is required if Session Manager 7.1 IPv6 features are to be enabled. Failure to ensure this will result in Avaya Breeze® platform nodes becoming unusable in this environment.

Note: Avaya Breeze® 3.6 or later is required if Session Manager 8.0.1 Routing Enhancements are to be enabled. Failure to ensure this will result in Avaya Breeze® platform nodes becoming unusable.

Refer to Session Manager documentation for complete information and implications of enabling these routing enhancements.

Upgrade compatibility and sequence

When installing updates to the Avaya Aura solution, it is important that the different components are upgraded in the correct order to ensure platform stability and manageability of the network as part of the upgrade process. Refer to Avaya Aura component release notes for the proper upgrade order. Avaya Breeze® platform can be upgraded at any time after Avaya Aura System Manager and Avaya Aura Media Server (if used) are upgraded. Please consult: https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml for the specific versions of products supported with this release of Avaya Breeze® platform.

Avaya Breeze® platform Release 3.8 is compatible with Avaya Aura Media Server Release 8.0 or 8.0.2.

Avaya Breeze® platform Release 3.8 is compatible with Authorization Service 3.8 and higher. Older versions of the Authorization Service for Breeze will no longer be compatible with Breeze platform release 3.8 and higher due to a version update of a dependent software component on the Breeze platform. Therefore, if currently using Authorization Service 3.6.0.3 or older, all nodes in the impacted Avaya Breeze® cluster should be upgraded simultaneously with the cluster in Deny New Service, refer to Method 2 in *Upgrading Avaya Breeze® platform*, https://downloads.avaya.com/css/P8/documents/101062804 . After the platform upgrade but prior to placing the cluster into Accept New Service, upgrade the Authorization service to Release 3.8.

If upgrading from Release 7.0 Avaya Aura ® System Manager to Release 8.1, be aware that if the data stored within the Avaya Breeze® platform cluster database for R3.2.x is to be retained, the cluster database backup operation must be performed prior to upgrade of the Avaya Aura ® System Manager to Release 8.1. See “Backing up a Cluster”, Chapter 3, in *Administering Avaya Breeze® platform* for information on how to complete this operation.

If you are coming from Release 7.0 Avaya Aura ® System Manager and have already upgraded the Avaya Aura ® System Manager to Release 8.1 prior to taking the cluster database backup, or if a significant amount of time has elapsed since the prior backup was taken on Avaya Aura® System Manager 7.0.x (data in prior archive is now stale and undesired), and the operational environment is now running the Avaya Aura® System Manager Release 8.1, contact Avaya Support for additional assistance.

Note: If one of the methods that you used to upgrade (see upgrade documentation for applicable uprade instructions) was via OVA or SDM and your snap-in relies on the data stored in the cluster database, you must restore the cluster database.

Disk Alarm notes

The System Overload Monitor has been enhanced to monitor the status of disks on an Avaya Breeze® platform server in addition to the current monitoring of CPU and memory. The monitored disks are the root directory disk /, /var, and /data. If any of these disks reaches a 90% usage level the system is placed in Overload, as it is when memory or CPU reaches a threshold of 80%. This condition causes an alarm OVERLOAD_100001 to be raised with the parameter disk, and the server is placed into Deny New Service state. If the disk reaches 95% of capacity, the node is placed in Extended Overload and alarm OVERLOAD_100003 is raised. Services identified to be associated with a high number of SIP sessions will be removed from service. When the disk is cleaned (manual clearing of files may be required) down to 75% of capacity (and CPU and memory are below the clearing threshold of 60%) the alarms are cleared and the system is placed back in Accept New Service.

New Alarm Details

New alarms (related to Authorization Service snap-in) are introduced in Avaya Breeze® platform 3.8. These alarms are raised when LDAP audit has been enabled (via the service attribute). The audit polls external LDAP providers (configured on Avaya System Manager) for connectivity issues and raises alarms if necessary. The new alarms are described below:

Event ID	Severity	Description	Action
GENERR1	Major	Any generic error caused when the Authorization Service tries to connect to an LDAP data source provisioned in SMGR.	Troubleshoot the issue by checking the appended root cause in the alarm description.
CONERR2	Major	A connection error occurred when the Authorization Service tried to connect to an LDAP data source provisioned in SMGR.	Rectify the connectivity between the LDAP source and the Breeze nodes.
SSLERR3	Major	An SSL error occurred when the Authorization Service tried to connect to an LDAP data source provisioned in SMGR.	Verify the LDAP related certificates that are currently deployed. Check if the LDAP CA certificate is properly installed in the cluster. For more information, you can also check the appended root cause in the alarm description.
CLR_GENERR1	Info	A generic error raised previously by the Authorization Service when trying to connect to an LDAP data source provisioned on SMGR, has been cleared.	No action.
CLR_CONERR2	Info	A connection error raised previously by the Authorization Service when trying to connect to an LDAP data source	No action.

		provisioned on SMGR, has been cleared.	
CLR_SSLERR3	Info	An SSL error raised previously by the Authorization Service when trying to connect to an LDAP data source provisioned on SMGR, has been cleared.	No action.

Logging API

A new method is introduced in the Logger API. Details as shown below.

```
public void logEventAlways(final String eventId, final Object... arguments)
```

This method is used to log events/alarms even when the node is in Deny New State.

Cluster Database notes

If use of the cluster database is required on an Avaya Breeze® platform cluster, it is recommended, in most cases, that deployment profile 2 or higher is used for fresh installations. For pre-existing deployments, it is recommended, in most cases, to increase your physical memory to 8GB or higher. Consult your snap-in documentation for disk sizing recommendations.

System memory on the Active Cluster Database node can go into swap on traffic when using the cluster database. When the cluster database is enabled, it consumes system memory depending upon the usage. It takes a minimum of 300 MB when no traffic is present. The overall memory consumption by the cluster database depends upon: the number of connections made from the snap-in; the number of nodes in the cluster; traffic rate; and database schema. The sustainable traffic rate also depends on the RAM size of the Avaya Breeze® platform nodes in the cluster. It is recommended to reduce the load on nodes hosting the cluster database. To accomplish this, make the following adjustments to the cluster. First assign the active cluster database to the same node as the active load balancer (if applicable). During upgrade, the active cluster database may need to move temporarily, but steps should be taken to adjust the roles of the cluster database post platform upgrade to follow this recommendation. Second, use the following table to determine the SIP load balancing weight to assign to each server in the cluster. This requires additional administration on the Local Hostname Resolution form for Session Manager. See High Availability Administration, in *Deploying Avaya Breeze® platform* for details about the administration required.

Number of servers in the cluster	2	3	4	5
Initial primary database server	50	25	16	12
Initial backup database server	50	25	16	13
Server 3		50	34	25
Server 4			34	25
Server 5				25

The exact memory requirements for the cluster database varies by snap-in. Consult your snap-in deployment guide for further details on their specific memory needs.

Media Operations notes

This scenario is specific to call scenarios where the party that answers a call may differ from the party that was originally called. For example, if the called party is a Vector Directory Number (VDN) on Communication Manager, where the associated vector destination does a redirect of the call to another party. Depending on how the vector is defined, the answering party reported to a snap-in may be different than the called party.

In Collaboration Environment 3.0 the distinction between the called party and answering party was ambiguous. This resulted in behavior where a media operation invoked on the called party was applied to the answering party, even if the answering party differs from the called party.

In Avaya Breeze® platform 3.1 and later, this distinction was refined so that media operations invoked on the called party are ineffective if the answering party differs from the called party.

Snap-ins that invoke media operations (e.g. play announcement, prompt and collect, speech search) on the called party may then encounter failures if the answering party is not the called party.

The desired behavior can be achieved by invoking media operations on the answering party.

WebRTC notes

The shared string for the authorization token is “Avaya Authorization Token.” Refer to the documentation for “How to use authorization token” and to the WebRTC sample application in the WebRTC SDK for details.

Whitelist Snap-in notes

On Breeze 3.4 and later, older versions of the Whitelist Sample Snap-in are no longer supported.

Zang SMS Connector Snap-in notes

In the Avaya Breeze® 3.5.x and prior, the Zang Outbound-only SMS Connector Snap-in was bundled with Avaya Breeze® platform. Going forward the Zang SMS Connector Snap-in supporting inbound and outbound SMS is available post GA as a separate PLDS download.

Flow control

It is important to avoid traffic congestion for a service that sends a burst of voice announcement requests through Avaya Breeze® platform. The current recommendation is no more than 375 phone numbers to be included per single request to this type of service. Each request must be staggered by 15 seconds or more between subsequent requests to the same service on the same Avaya Breeze® platform instance. Empirical testing has shown that a reliable minimum delay for 10,000 requests using one Avaya Breeze® platform is 15 seconds. A lower delay value is not recommended because it increases the probability of encountering performance-related problems.

Additional consideration should be given when the sum of requests targeted for the voice announcements exceeds the maximum port allocation for a single instance of the Avaya Aura Media Server. The Avaya Aura Media Server virtual machine bundled with Avaya Breeze® platform is maximum rated at 1100 ports. A single Avaya Aura Media Server would be expected to service 1,000 announcements over a period of five minutes and therefore 2,000 announcements would be serviced over 10 minutes. Given this guideline, five Avaya Aura Media Server instances will be required at a traffic level of 10,000 voice announcement requests serviced over a ten minute time period. The same traffic distribution guidelines as discussed above apply here as well.

If the phone numbers specified in the voice announcement request contain non-SIP devices such as H.323 endpoints or non-SIP trunk resources, be sure to verify this configuration to ensure you have the needed Digital Signal Processors (DSP) resources required to support a simultaneous voice announcement request to this set of users.

The following formula can be used to estimate the number of Avaya Aura Media Server instances required to support a particular burst application.

MaxSimultaneousRequiredLicenses = (((AnncLength + MaxDelayToAnswer)/FCDelay) * (CollectionSize))*NumberOfLicensesPerCall)

TotalAMSInstances*=ceiling((MaxSimultaneousRequiredLicenses)/(AMSMaxLicenseThreshold))

AnncLength = full length of the recorded announcement in seconds.

MaxDelayToAnswer = anticipated max ringback delay prior to answer in seconds.

FCDelay = Flow Control Delay, which is the time between simultaneous collection bursts to an Avaya Breeze® platform instance in seconds (current recommendation is 15 seconds or more).

CollectionSize = For an outcalling burst application this number represents the total number of users defined within a single simultaneous request for voice announcements to an Avaya Breeze® platform instance.

AMSMaxLicenseThreshold = the default threshold is 825 (75% of current session maximum).

NumberOfLicensesPerCall = 2 (number of active sessions per call; each session uses 1 license).

*In summary, the **TotalAMSInstances** is the "rounded up" value of the total number of simultaneous licenses required, divided by the license threshold administered on a single Avaya Media Server virtual machine. See the example below for further clarification.

For example:

Using the sample service, MultiChannel Broadcast, send 10,000 voice 45-second announcements to individual phone numbers within or off enterprise. In this type of example, assume it will take no more than 15 seconds for any user to answer the calls generated from this application and a single request includes 250 phone numbers, therefore 40 requests are required to reach 10,000 phone numbers in total.

AnncLength=45 seconds

MaxDelayToAnswer=15 seconds

FCDelay = 15 seconds

CollectionSize= 250

MaxSimultaneousRequiredLicenses = (((45+15)/15)*250)*2 = 2000

TotalAMSInstances = ceiling (2000/825) = 3

request1=[phone1…phone250]; request2=[phone251…phone500], …,
request40=[phone9750…phone10000]

Each request per Avaya Breeze® platform instance would still need to be staggered by 15 seconds.

In this example, a total of three Avaya Aura Media Servers and one Avaya Breeze® platform instance could service the request for 10,000 voice announcements within 10 minutes. Note: a larger collection, longer answer delay, and/or announcement length requires additional Avaya Aura Media Server resources.

Callbacks for Media Operations

Some behaviors have changed related to media callback listener methods to improve consistency in the media portions of the API (including voice XML and speech search). The original and changed behaviors are:

1. Invoking stop on a prompt and collect media operation.

   ORIGINAL BEHAVIOR: Two invocations of MediaListener methods are made, one to the playCompleted callback method with a cause of STOPPED, and one to the digitsCollected callback method with a cause of STOPPED.

   NEW BEHAVIOR: A single invocation is made to the digitsCollected method with a cause of STOPPED. This new behavior aligns better with the behavior that occurs when a prompt and collect operation ends after playing prompt and collecting digits.

2. Invoking stop on a send digits operation.

   ORIGINAL BEHAVIOR: The invocation of stop has no effect, and the send digits operation continues to completion as if stop were NOT invoked. Upon completion no invocation of the MediaListener's sendDigitsCompleted method occurs.

NEW BEHAVIOR: The invocation of stop still has no effect. However, upon completion of the send digits operation, the sendDigitsCompleted method is invoked with a cause of COMPLETE. This new behavior better reflects what has actually taken place.

3. A party drops/is dropped from a call under the following circumstances:

    a. The call termination policy is set to NO_PARTICIPANT_REMAINS.

    b. A media operation is active on the dropped party.

ORIGINAL BEHAVIOR: An invocation of the appropriate MediaListener callback method occurs for the operations play, prompt and collect, collect, and record. For other media operations, no listener callback methods are invoked. NOTE: The listener interface that is implemented by a snap-in for most media operations is MediaListener. For voice XML and speech search, the listener interfaces are VoiceXMLDialogListener and SpeechSearchListener, respectively.

NEW BEHAVIOR: An invocation of the recordCompleted method occurs for an active record operation. No invocation of callback methods occurs for other media operations. This new behavior better matches the behavior that occurs when a call ends.

General Operational Changes/Frequently Asked Questions

1. **Java API change** behavior from 3.2 -> 3.3

   The return value from the Java API InetAddress.getHostName() on an Avaya Breeze® platform node has changed from returning an FQDN (e.g., myhost.example.com) to returning the host's name (myhost). If the FQDN is desired, use InetAddress.getCanonicalName()."

2. **Authorization service** behaviour – The Avaya Breeze® platform Authorization Service does not support SAML Single Logout.
   The Avaya Breeze® platform Authorization Service acts as an SAML Service Provider when trying to authenticate end-users against an Identity Provider. Authentication is initiated by using an SP initiated SSO exchange. The Authorization Service then optionally creates a session for the user, and redirects the user back to the Client snap-in with an "authorization code". For the current release, SP initiated Single Logout is not supported.

3. **Authorization service** behaviour – After authenticating the user, the following error is seen on the browser: Client authentication failed. Session validation failed.

   Resolution:

   - On System Manager click **Elements> Avaya Breeze®> Cluster Administration.**
   - Select the Cluster where Authorization Service has been installed.
   - Select the "Certificate Management" tab.
   - Click on "Update/Install Identity Certificate (Authorization Service)"

Avaya Breeze® platform 3.8 port changes

There are no notable changes to port usage in Avaya Breeze® platform 3.8.

Avaya Breeze® platform traceMessage message tracer tool

Prior to release 3.3, individual execution of traceHTTP, traceBus and traceSIP were required. With traceMessage, the ability to trace and view multiple protocols within the same tool is now supported.

New with traceMessage is the ability to enable and show installed snap-in logs as well as trace AAMS media control messages over HTTPs.
NOTE: Although media server messages are HTTP messages, the trace tool generally treats media server messages separately from other HTTP tracing messages. Media server tracing is generally most useful when combined with SIP tracing. The SIP messages provide the context within which the media server messages are generated for a given call.

As with the previous trace tools, traceMessage can be performance impacting depending on the current traffic levels on the Avaya Breeze® platform server.

The Filter options can take a regular expression. Filters are also available by pressing 'f' in the application.

WARNING: traceMessage may use high CPU and memory in a busy Avaya Breeze® platform server. The trace will stop displaying packets after capturing 10000 messages.

Usage examples:

- To start a new capture, run 'traceMessage' without arguments and then press 's':
  `$ traceMessage`
- To filter messages from/to 1.1.1.1 and 2.2.2.2:
  `$ traceMessage -i "1.1.1.1|2.2.2.2"`
- To analyze previously captured files for SIP, HTTP, AAMS and the call processing logs:
  `$ traceMessage call_proc.log tracer_asset.log mediaServer_http.log niginx_http.log`
- To filter SIP messages containing 'Avaya' in the 'User-Agent' header field:
  `$ traceMessage -g "User-Agent=Avaya"`
- To filter SIP sessions that got a '487 Request Terminated' response:
  `$ traceMessage -o "487 Request Terminated"`

New Avaya Breeze® platform External Authorization SDK

With the introduction of Avaya Breeze® platform Authorization Service support with Oceana 3.3 / Avaya Breeze® platform Client SDK 3.2 role based authorization used by Avaya Breeze® platform Client SDK’s Identity Management Services Package was removed and this package was marked obsolete. This created a solution gap for 3rd party developers wishing to create Oceana based applications. The new External Authorization SDK bridges this gap with the support of:

Authorization Code Grant Type

- Both the Application and the user are authenticated. It is a redirect-based flow.
- Application does not handle the user’s credentials. It redirects the user’s browser to the Avaya Breeze® platform Authorization Service (AS) for validation of credentials.
- Once validated by the Authorization Services it redirects the browser back to the application with an authorization code, which the application can then exchanges for an access token.

Authorization Code Grant Type can enable SAML-based authentication, which could include Multi-Factor Authentication (MFA).

The External Authorization SDK can be used with Avaya Breeze® platform Authorization Services release 3.3, 3.4,3.4 SP or 3.5, 3.5 SP, 3.6, 3.7 and 3.8

Security -- Spectre/Meltdown

For more information on Spectre/Meltdown mitigation refer to PSN020346u.

- To mitigate the Meltdown and Spectre vulnerabilities, the processor manufacturers and operating system developers must provide software patches to their products. These are patches to the processors and operating systems, not to Avaya products.

- When these patches are received by Avaya, Avaya will test these patches with the applicable Avaya products to determine what, if any, impact these patches will have on the performance of the Avaya product.
- Avaya is reliant on our Suppliers to validate the effectiveness of their respective Meltdown and Spectre vulnerability patches.
- Avaya's test effort is targeted towards reaffirming product/solution functionality and performance associated with the deployment of these patches.
- The customer is responsible for implementing, and the results obtained from, such patches.
- Although Avaya Breeze® platform performance impact is negligible, customers should be aware that implementing these patches may result in performance degradation.

Enhanced Security with LDAPs Connections

Issue: Avaya Breeze® platform applications that were previously able to successfully connect via LDAP over a secure connection may no longer be able to do so.

Background: Beginning with Avaya Breeze® platform 3.6.0.0, endpoint identification has been enabled on LDAP secure TLS connections. This may necessitate the need to generate a new identity certificate for the LDAP server that includes the server's Fully Qualified Domain Name (FQDN) or IP Address.

How to identify:

1. In the Avaya Breeze® platform application log for Authorization (/var/log/Avaya/services/AuthorizationService/AuthorizationService.log), check for the following exception:

```
[Root exception is javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: No subject alternative names present]
Caused by: java.security.cert.CertificateException: No subject alternative names present
at com.ibm.jsse2.util.b.b(b.java:104)
at com.ibm.jsse2.util.b.a(b.java:88)
at com.ibm.jsse2.aD.a(aD.java:165)
at com.ibm.jsse2.aD.a(aD.java:168)
at com.ibm.jsse2.aD.a(aD.java:211)
```

Recommended Solution:

1. First, inspect the current identity certificate on the LDAP server using one of the following mechanisms:
   a. System Manager Trusted Certificates provisioning
      1. On System Manager navigate to **Services > Inventory > Manage Elements**.
      2. Select the Avaya Breeze® platform node and choose **More Actions> Manage Trusted Certificates.**
      3. Choose Add, then Import using TLS.
      4. Enter the IP address or FQDN of the LDAP server, and port 636.
      5. Push **Retrieve**.
      6. Inspect the certificate details.
   b. OpenSSL command line tool.
   c. Login to an Avaya Breeze® platform server using the cust login, or to any other machine that has the OpenSSL tools installed:
      1. Run the following command, substituting your actual LDAP FQDN or IP address for MY_LDAP_FQDN_OR_IP:

         ```
         echo | openssl s_client -showcerts -servername <MY_LDAP_FQDN_OR_IP> -connect <MY_LDAP_FQDN_OR_IP>:636 2>/dev/null | openssl x509 -inform pem -noout -text
         ```

      2. Inspect the certificate details.

2. Check the certificate for the presence of the LDAP server's FQDN in the CN or in the Subject Alternative Name (SAN) fields. The LDAP server name or IP address must match what is in the CN or SAN. Additionally, if FQDN was used, DNS must be setup with this FQDN and corresponding IP.
3. If there is not a valid FQDN or IP address in the certificate, generate a new certificate with valid FQDN or IP address (FQDN recommended) in the CN or SAN filed and provision it on your LDAP server.
4. Navigate to **Users> Directory Synchronization > Sync Users** and check the datasource. It must be configured with the exact FQDN or IP address used in the certificate.
5. If required, import either the LDAP server's certificate or the Certificate Authority (CA) certificate (recommended) as a trusted certificate for Avaya Breeze® platform by completing the process specified in 1a above. If the new certificate is signed by the same CA as had signed the previously used certificate, and if that CA certificate was previously provisioned as trusted by Avaya Breeze® platform, this step should not be required.

Refer to https://developer.ibm.com/answers/questions/475181/how-to-fix-this-ldap-ssl-error-javasecuritycertcer.html and https://www.oracle.com/technetwork/java/javase/8u181-relnotes-4479407.html?printOnly=1 for more detail on this enhanced security setting.

Authorization Service SAML authentication support matrix

Authorization Service v 3.7 and 3.8

Authentication Mechanism	Windows 2012 Domain Controller	Windows 2016 Domain Controller
LDAP	Yes	Yes
SAML - Password Protected Transport	Yes	Yes
SAML – Integrated Windows Authentication	Yes	Yes
SAML - Kerberos	No	Yes