Avaya Experience Portal 8.1.2 Release Notes

Release 8.1.2
Issue 1.1
October 2022

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.

Licenses

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

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

License types

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.

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”).

Copyright

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

Virtualization

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

Third Party Components

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

Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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.

Trademarks

Avaya, the Avaya logo, Avaya Experience Portal, Avaya Aura® Communication Manager, and Avaya Orchestration Designer are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

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

Document changes

Issue	Date	Description
1.0	4-Oct 2022	Release of AEP 8.1.2 on 4-Oct 2022
1.1	12-Oct 2022	Add new Known Issue

Introduction

This document provides late-breaking information to supplement Avaya Experience Portal software and documentation. For updated documentation, product support notices, and service pack information, go to the Avaya Support site at http://support.avaya.com. Additionally, updated on-line help that is accessed through the Avaya Experience Portal management web pages may also be available on the Avaya Support site at http://support.avaya.com.

Key Notifications

Security enhancements delivered in AEP/AOD 8.1.2 **may require customer action** as detailed below

Summary	Details/Recommendations	Impact if no action taken
As part of AEP 8.1.2. upgrade from AEP 8.0/8.1/8.1.1, the local WebLM server is upgraded from WebLM 7.1 to WebLM 8.1. If AEP is using Local WebLM for licensing, then the license will be **invalidated** due to the WebLM Host ID changing between WebLM 7.1 and 8.1. Also, the WebLM admin password is reset back to default and any additional WebLM administrator users are deleted.	Old license is stored in: /opt/Avaya/InstallLogs/WebLM71/OldLicense Supply this license along with new HostID to Avaya Support. Avaya will issue a new license using the new Host ID. WebLM admin user password is set back to default and any additional WebLM users are deleted.	AEP goes into grace mode licensing and will be unlicensed after 30 days. Use default WebLM admin password to logon to WebLM UI.
Upgrade from AEP 8.0/8.1/8.1.1 with 1024-bit x509 security certificates to AEP 8.1.2+ will require 2048-bit x509 security certificates to be reapplied as the Crypto Policy on RHEL OS in 8.1.2 will not support 1024-bit x509 level security certificates.	In AEP 8.1.2 the crypto level setting on RHEL OS has been set to DEFAULT level which is the recommended level to secure the platform. At this DEFAULT level 1024-bit x509 security certificates can no longer be supported and should be removed and replaced with industry recommended 2048-bit x509 security certificates prior to upgrading to AEP 8.1.2. Note: Where custom certificates have not been imported and the default certificates that come with AEP deployment are still in place are already created with 2048-bit x509 security certificates and no changes are required to upgrade	Failure to plan and remove any 1024-bit x509 security certificates from AEP configuration prior to upgrading will result in loss of features and services failing to start.
Upgrade to AEP 8.1.2+ introduces more stringent JS syntax rules for the VXML/CCXML Interpreter that	The MozJS JavaScript interpreter engine in MPP has been upgraded from MozJS 17 to MozJS 52.	As a precaution and to prepare, the recommendation would be to perform a complete sanity of all code paths in all CCXML and VXML Applications. Special

may require existing applications to be modified	It has been identified that this upgraded JS interpreter version enforces stricter JavaScript syntax rules. This can cause issues for existing Applications that did not have issues when running on the previous version of MozJS. Below is an example of a known issue. Note, there could be other JS syntax enforcement changes. **Known Issue:** <assign name="testSet" expr="Set(JSON.parse(setObject))"/> This assign element in VXML worked in MozJS 17 however it throws the following error in MozJS 52. ECMA Exception:: TypeError: calling a builtin Set constructor without new is forbidden This causes the Application to exit. The resolution of this issue was to use the new keyword when calling the Set constructor. <assign name="testSet" expr="new Set(JSON.parse(setObject))"/>	attention should be given to those Applications that heavily utilize JavaScript.
Upgrade to AEP 8.1.2+ / AOD 8.1.2+ will require AOD based applications that invoke the Axis 2 APIs or Axis2 PDC on web services or EPM services on the EPM server to be rebuild using AOD 8.1.2 to maintain functionality. AOD applications that do not use this functionality are not impacted.		
If using Standalone WebLM or SMGR hosted WebLM and using https for licensing, AEP 8.1.2 will not be able to acquire licenses from the WebLM server without trusted certificates being installed on AEP	If the EP web admin > Security > Licensing > License Server URL is https, AEP 8.1.2 requires that the public certificates of the CA that issued the WebLM servers identity certificate are uploaded to EP as a trusted certificate. Installing a Platform type trusted certificate on AEP is required. The required certificate chain can be installed in EP web admin > Security > Certificates > Trusted Certificates using the import option and specifying the URL of the WebLM server. The Experience Portal Administration guide has details on this process. This allows EPM's WebLM client to communicate securely with the WebLM server. Note: If the coresident WebLM server on EPM is being used, no trusted certificates need to be installed on AEP to establish communications with the WebLM server – an automatic trust relationship is setup by AEP.	AEP will not be able to acquire licenses from the WebLM server and the license will go into grace period.

Installation

Installing the release

AEP 8.1 introduced a new installer mechanism. This section covers this procedure.

Note: This section covers both fresh installation of AEP 8.1.2 and upgrades from a previous AEP 8.0 and 8.1.x version that was released (i.e. 8.0.0.0.1217 with any available patches or 8.1.0.0.0233 with any available patches or 8.1.1.0.0122 with any available patches).

General Notes

- RHEL 7.8+ and 8.2+ version supported as well as AVL (based on RHEL 8.4)
- Customer must either install RHEL 7/8 Server and configure yum repo (using RHEL iso) or use AVL
- Installer then installs required RPMs and installs one of the following:
    - Primary EPM (Standalone)
    - Auxiliary EPM
    - MPP (Standalone)
    - Primary EPM and MPP on single server (co-resident)
- A non-root user account with known password MUST be created prior to running installation. PVI Checker in AEP Install checks for a non-root account.
- Firewall must be disabled (Installer will disable firewall if enabled)
- FIPS must be disabled.
- EPM must have chronyd (NTP) configured.

Fresh RPM Install instructions

1. Install RHEL 7.x or RHEL 8.x or AVL from DVD/ISO
2. Disable FIPS as per FIPS 140-2 Support
3. Disable firewall.
    i. systemctl stop firewalld
    ii. systemctl disable firewalld
4. Configure chronyd (NTP) on Server designated as Primary EPM.
5. If not using AVL then set up yum repo from RHEL 7/8 DVD or ISO:
    i. mkdir /mnt/cdrom
    ii. DVD: mount -t auto /dev/cdrom /mnt/cdrom
    or ISO: mount -o loop rhel-server-8.2-x86_64-dvd /mnt/cdrom
    i. cp /mnt/cdrom/media.repo /etc/yum.repos.d/
    ii. chmod +rw /etc/yum.repos.d/media.repo
    iii. Run one of the following:

    RHEL7: `echo -e "baseurl=file:///mnt/cdrom\nenabled=1\ngpgcheck=0" >> /etc/yum.repos.d/media.repo`

    RHEL8: `echo -e "baseurl=file:///mnt/cdrom/BaseOS\nenabled=1\ngpgcheck=0\n[InstallMedia-AppStream]\nname=Red Hat Enterprise Linux 8 - AppStream\nmetadata_expire=-1\nenabled=1\nbaseurl=file:///mnt/cdrom/AppStream/\ngpgcheck=0\n" >> /etc/yum.repos.d/media.repo`
6. Mount the **AEP-8.1.2.0.0202.iso** file on Linux server.
    One method to do this is:
    i. Copy AEP-8.1.2.0.0202.iso file to /tmp folder on Linux server
    ii. Run command: mkdir -p /mnt/aep812
    iii. Run command: mount -o loop AEP-8.1.2.0.0202.iso /mnt/aep812
7. Run the following command to install EPM or MPP:

i. cd /mnt/aep812
ii. bash aepinstall.sh

8. Select option to install either:
   i. Primary EPM
   ii. Auxiliary EPM
   iii. Standalone MPP
   iv. Single Server - Primary EPM and MPP
9. Install time of EPM is approximately 20 minutes. MPP Install time is approximately 5 minutes.
10. If FIPS is required, then enable FIPS as per FIPS 140-2 Support
11. For EPM: Logon to Web admin using https://<EPM_IP>/VoicePortal with Web admin user and password entered during installation

Upgrades

For upgrades see the document ***Upgrading to Avaya Experience Portal 8.1*** *(*https://downloads.avaya.com/css/P8/documents/101083233*).*

Upgrade from AEP 8.0/8.1/8.1.1 (WebLM 7.1) to AEP 8.1.2+ (WebLM 8.1) - Local WebLM License changes
Upgrading an AEP server with Local WebLM co-resident from AEP 8.0/8.1/8.1.1 to AEP 8.1.2+ will result in a new WebLM Host ID being created that will require the existing WebLM license to be re-hosted on PLDS. Post upgrade, the AEP will go into a 30-day grace mode until the re-hosted license is applied. This is only required if Local WebLM co-resident server is used for AEP licensing. Reference PLDS re-hosting document (https://support.avaya.com/public/downloadFile.jsp?file=/resources/sites/AVAYA/content/live/SOLUTIONS/346000/SOLN346998/en_US/PLDS%20-%20Rehost.pdf)
Local WebLM admin user account password is set to default and any additional WebLM users are deleted as part of the WebLM 7.1 to WebLM 8.1 upgrade.

Known Installation Issues

1. Installing EPM patch procedure has changed due to support of umask 027. When the EPM ".tar.gz" file is copied over to the EPM, in order to deploy the patch, and the tar is extracted. It will not have correct permissions to run. The setup.sh detects this and prints out the commands that are required to resolve this issue. The permissions of the entire directory tree that contains the file will need to be changed. e.g.

   If EPM tar.gz file is extracted to directory: /tmp/patch/ then the following commands need to be run:

   ```
   chmod +orx /tmp
   chmod +orx /tmp/patch
   ```

2. OVA deployments fail on older versions of VMWare. Make sure you have patched VMWare servers to the latest release.

   OVA deployments have been verified on:

   ESXi 6.5 P04 *
   ESXi 6.7 P01 *
   ESXi 7.0 Update 2a

   * As of October 15, 2022, VMWare is Ending General Support for vSphere 6.5 and vSphere 6.7

3. Install will fail with FIPS enabled.

   Workaround: Disable FIPS before running any fresh installs or upgrades.

Important: Before installing or upgrading Avaya Experience Portal, please review the **Known Issues** section in this document for issues that are not addressed in the product documentation.

For detailed installation and upgrade procedures, see the Avaya Technical Support Web site https://support.avaya.com and the document titled ***Implementing Avaya Experience Portal on multiple servers*** *(*https://downloads.avaya.com/css/P8/documents/101083239*) or* ***Implementing Avaya Experience Portal on a single server*** *(*https://downloads.avaya.com/css/P8/documents/101083237*)*. For upgrades see the document ***Upgrading to Avaya Experience Portal 8.1*** *(*https://downloads.avaya.com/css/P8/documents/101083233*).*

For detailed OVA installation and upgrade procedures, see the Avaya Technical Support Web site https://support.avaya.com and the document titled ***Deploying Avaya Experience Portal in an Avaya Customer Experience Virtualized Environment*** *(*https://downloads.avaya.com/css/P8/documents/101083235*).*

For information about patches and product updates, see the Avaya Technical Support Web site https://support.avaya.com.

Troubleshooting the installation

For detailed troubleshooting procedures, see the Avaya Technical Support Web site https://support.avaya.com and the document titled ***Troubleshooting Avaya Experience Portal*** *(*https://support.avaya.com/css/P8/documents/101078562*)*.

Product compatibility

Note the following limitations.

Application	Compatibility Description	Recommendation
Proactive Outreach Manager (POM)	POM 4.0 SP1 is the minimum supported release with AEP 8.1. POM 4.0.1 Patch 2 is the minimum supported release with AEP 8.1.1 POM 4.0.1 Patch 2 currently does not support FIPS (PSN PSN005975u) **POM 4.0.2*** is the minimum supported release with AEP 8.1.2.	Verify compatibility from the matrix referenced below
Intelligent Customer Routing (ICR)	ICR 8.0 is supported with upgrades from AEP 8.1 to AEP 8.1.1. ICR 8.0 is not supported with a fresh installation of AEP 8.1.1. ICR 8.0.0.1 Service Pack targeted to launch in Feb 2022 will be the minimum supported release for fresh installation with AEP 8.1.1 **ICR 8.0.0.2*** is the minimum supported release with AEP 8.1.2. ICR 8.0.0.2 is Targeted for Launch in Nov 2022	Verify compatibility from the matrix referenced below
Avaya Orchestration Designer (AOD)	AOD backward compatibility is supported with AEP 8.1.2. Any API that consumes AEP axis 2 Web services will require **AOD 8.1.2*** and will have to be re-evaluated and recompiled when upgrading to AOD 8.1.2	Verify compatibility from the matrix referenced below

* Support for Log4j v2 delivered in Experience Portal 8.1.2, Orchestration Designer 8.1.2 (Runtime), POM 4.0.2, and ICR 8.0.0.2 requires that all the listed applications be upgraded to the highlighted releases. The individual applications will not work on a lower release (example > POM 4.0.1 will not work with EP 8.1.2, POM 4.0.2 will not work with EP 8.1.1) as they are not backwards compatible!

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

File list

Verify Download of Avaya Experience Portal 8.1.2 software using SHA256 Checksum

All Avaya Experience Portal 8.1.2 software packages have an associated file that contains the SHA256 checksum of the corresponding file. The File list below also contains the SHA256 checksum. This allows you to verify the validity of the downloaded package by using the following procedure:

1. Login to the Linux system as a root privilege user and perform the following commands:

2. Use “sha256sum” command to generate a SHA256 hash against the associated file.

   sha256sum AEP-8.1.2.0.0202.iso

3. Compare the calculated hash from the above step with the published SHA256 checksum in the tables below. The SHA256 hash should be the same value to ensure the ISO/OVA images are not corrupted

File list - Avaya Experience Portal 8.1.2 software

Filename	SHA256 Checksum	File size	Version number
AEP-8.1.2.0.0202.iso	ebded6a52dddc3d8dabe0547af22a82737f64602255e032a79e1c1c19b0f18de	1,465,233,408	8.1.2.0.0202
AEP-8.1.2.0.0202.sig	7f0ce5e59078b5347e7947fbaebbfb081a5e667f94e010ba128d44aa87a08404	256	8.1.2.0.0202
Avaya_Public_Certificate_2030.crt	a79ea87dc2ab3c0e0b090db819909357cabb1eff57a95b7a06be35c3d1007202	1842	N/A

File list - Avaya Experience Portal 8.1.2 OVA software

Filename	SHA256 Checksum	File size	Version number
ExperiencePortal-Primary-EPM-8.1.2.0.0202.ova	a641ffdd0c6266145f2c66a6aa01f55d5b581bc019388cd7a8b1725c1badb695	4,975,538,176	8.1.2.0.0202
ExperiencePortal-Primary-EPM-8.1.2.0.0202.ova_checksum.sig	dc35fed813c09c037b8b95715cfe59478429204411cba34aab2ac9f8c823740b	256	8.1.2.0.0202
ExperiencePortal-Auxiliary-EPM-8.1.2.0.0202.ova	beabcae3b099d4b9c5bcc794215678c718687624fe8778382e70883b80ff7f75	4,975,538,176	8.1.2.0.0202
ExperiencePortal-Auxiliary-EPM-8.1.2.0.0202.ova_checksum.sig	5555af25c4c496df9e8a33f6c697717bf67c62709fe371c63f790021d309228a	256	8.1.2.0.0202
ExperiencePortal-MPP-8.1.2.0.0202.ova	c17dd7a687b0082cc324578a007493853a05c9d92a137b4168e6e7cd8cc6c3a9	4,113,406,976	8.1.2.0.0202
ExperiencePortal-MPP-8.1.2.0.0202.ova_checksum.sig	570b08947d7eb3ed33bcda7b98ada61b3d13945c22bf54b0c33b71420bce4d4a	256	8.1.2.0.0202
Avaya_Public_Certificate_2030.crt	a79ea87dc2ab3c0e0b090db819909357cabb1eff57a95b7a06be35c3d1007202	1,842	N/A

File list - Avaya Experience Portal 8.1.2 zero-day patch

Filename	SHA256 Checksum	File size	Version number
EPM_8.1.2.0.0328.tar.gz	283219d04cf8eeeba5ff20734c9f9bf7cc2773010ba97bf44e51e81d0323fcb7	54,385,643	8.1.2.0.0328
8.1.2.0.0328.tar.gz	afd776063c18b04e4c89adece913078beac6aff460222ebc2ed1350e0caef1d6	28,789,256	8.1.2.0.0328
8.1.2.0.0328.tar.gz.sig	06970a517c336e2fe6aa1956bbdc58f099fb4df8915a3011e61d08753712d96c	256	8.1.2.0.0328
Avaya_Public_Certificate_2030.crt	a79ea87dc2ab3c0e0b090db819909357cabb1eff57a95b7a06be35c3d1007202	1,842	N/A

File list - Avaya Experience Portal 8.1.2 Post GA patch

Filename	SHA256 Checksum	File size	Version number

File list - Avaya Enterprise Linux for Avaya Experience Portal 8.1.2 software

Filename	SHA256 Checksum	File size	Version number
AvayaLinux-RH8.4.64-AV04EP8.27Jun22.132645.iso	fa75e8758fd6d15752d621047113661f4887e31bbc86fae27c11d8ae5c16f64c	1,501,327,360	RH8.2.64-AV21EP8
AvayaLinux-RH8.4.64-AV04EP8.27Jun22.132645.SCRIPT.sh	12f9c324d38aed9470e3be6bd6e41dddd8de762feb8cb703b72f40a265e8ab58	44,885	RH8.2.64-AV21EP8
AvayaLinux-RH8.4.64-AV04EP8.27Jun22.132645.sha256.sig	415d32c894ef8a752d4c6f5c65c9337f078e6cd918f03580031a213813617100	256	RH8.2.64-AV21EP8
Avaya_Public_Certificate_2030.crt	a79ea87dc2ab3c0e0b090db819909357cabb1eff57a95b7a06be35c3d1007202	1,842	N/A

File list - July AVL Security patch

Filename	SHA256 Checksum	File size	Version number
epavl-8.x.x.0.2207.tar.gz	142702a5fe2e607e1aad8b461d8eb5d6f98c89419472cad26eea0af8c2a7e462	581,040,171	2022-07
epavl-8.x.x.0.2207.sha256.sig	764dc25dffb419b5c3b2dfff0d0e47ccf165d84ea6a03b6e024c3f8e09d67c48	256	2022-07
epavl-8.x.x.0.2207.readme.txt	38751f6deb5834ef98e43f0457971de18f043f213c922ddfeb3d5b116a65a21c	70,571	2022-07
Avaya_Public_Certificate_2030.crt	a79ea87dc2ab3c0e0b090db819909357cabb1eff57a95b7a06be35c3d1007202	1,842	N/A

To support upgrades for systems that were created on earlier versions of AEP 8.x, the most recent AVL security patch must be used to put the system into the proper state to support upgrades to 8.1.2.

bash ./setup.sh -v 8.1.2

This needs to be done prior to upgrading to AEP 8.1.2 to install the required prerequisite packages on the system.

See the patch readme.txt for additional information.

All Avaya Enterprise Linux for Avaya Experience Portal 8.1.2 software packages are protected via code signing. The SHA256 hash is generated and signed by the Avaya File Signing Authority for each Avaya Enterprise Linux for Avaya Experience Portal 8.1.2 software package. The following describes the steps to validate the SHA256 hash and digital signature.

Software Package name	Steps to validate the SHA256 hash and digital signature
AvayaLinux-RH8.4.64-AV04EP8.27Jun22.132645.iso	This is the Avaya Linux ISO Image. Login to the Linux system as a root privilege user and perform the following commands: 1. Use "sha256sum" command to generate a SHA256 hash against the Avaya Linux ISO Image: **AvayaLinux-RH8.4.64-AV04EP8.27Jun22.132645.iso** 2. Compare the calculated hash from the above #1 step with the published SHA256 checksum on support.avaya.com. The SHA256 hash should be the same value to ensure the ISO/script image is not corrupted. 3. The following steps are to validate the SHA256 hash signature: • First extract the public key from the certificate that signed the SHA256 hash to "pubkey.pem". **openssl x509 -pubkey -noout -in Avaya_Public_Certificate_2030.crt > pubkey.pem** • Create the SHA256 of the ISO **sha256sum AvayaLinux-RH8.4.64-AV04EP8.27Jun22.132645.{SCRIPT.sh,iso} > AvayaLinux-RH8.4.64-AV04EP8.27Jun22.132645.iso.sha256** • Verify the SHA256 hash signature using the public key "pubkey.pem" and SHA256: **openssl dgst -sha256 -verify pubkey.pem -signature AvayaLinux-RH8.4.64-AV04EP8.27Jun22.132645.sha256.sig AvayaLinux-RH8.4.64-AV04EP8.27Jun22.132645.iso.sha256** "Verified OK" from the above command indicates the SHA256 hash signature is valid.

File list - Avaya Orchestration Designer 8.1.2 software

Filename	SHA256 Checksum	File size	Version number
AOD_8_1_2_1101.iso	**be6c2dbfdba4f951784fc8db92f065409a18c5a24235c344e098aac69e9c0506**	**1,941,231,616**	**8.1.2.1101**
AOD_8_1_2_1101-iso-checksums.txt	**5934879e5f882c49faa2d273685d7e25196ac92bd826b0b83877eabceaebee15**	**376**	**8.1.2.1101**
AOD_8.1.2.1101_202209131323.jar	**da3f29c7dffdc6fd55c4cd30a7d476cd930600a8e4521137a00241b968868612**	**101,846,178**	**8.1.2.1101**
OD_8_1_2_1101.pdf	**2b705d5fbd952f687ca74bc36c57233e1a67e230d5345c70dd3973a8d7e12cee**	**440,046**	**8.1.2.1101**
AOD_DevGuide.pdf	**0eab20fea0d784ce7b2e825e46d0360e0c2eb6416515aed7c843a4e8b34fc5ac**	**5,071,557**	**8.1.2.1101**
AOD_GettingStarted.pdf	**94ab166a4d0a66c8615354e4745b33c313fa69cf9f39583c6fd937a82274e0c4**	**369,354**	**8.1.2.1101**

Backing up the software

Important: Before starting an upgrade, you should back up your existing Avaya Experience Portal database. In many cases the upgrade procedure requires you to take a backup to preserve your existing data. Additionally, if the upgrade fails for any reason you will need this backup to restore your system to its prior state.

For detailed upgrade and backup procedures, see the Avaya Technical Support Web site https://support.avaya.com and the document titled ***Upgrading to Avaya Experience Portal 8.1*** *(*https://downloads.avaya.com/css/P8/documents/101083233*)*.

Functionality not supported

Experience Portal has not been formally tested with Avaya Appliance Virtualization Platform (AVP) or Solution Deployment Manager (SDM)

Google Dialogflow Issue: Dialogflow connectivity slow detection of dead TCP connections

AAEP uses Google gRPC libraries for communication with Google Dialogflow. It was observed during testing that these libraries could take up to fifteen minutes to detect a dead TCP connection. This would result in significant call disruption for a short network outage.

To speed up the detection of TCP dead connections to around eight seconds, the following Red Hat Linux configuration is required on the AAEP MPP server:

1. Log on using a secure shell session (SSH) to the Avaya Enterprise Linux system as a user with root privileges
2. Open the file: /etc/sysctl.conf
3. Add the following lines to the end of this file

   ```
   # Avaya MPP, Speed up detection of Dead TCP connection to approx. eight seconds
   net.ipv4.tcp_retries2=6
   ```
4. Reboot the MPP server for settings to take effect.

Note: Google Dialogflow capacity is increased from 450 concurrent calls to a maximum limit of 1500 concurrent calls active to Dialogflow per MPP. This does not impact any other call or speech vendor capacity.

What's new

The following table lists the enhancements in Avaya Experience Portal 8.1.2 and is cumulative since the last major/minor release showing the most recent release first and oldest release last (currently includes features delivered in 7.2, 8.0, 8.1 and 8.1.1).

**New in AEP 8.1.2*

Enhancements	Description
Branding	• Experience Portal 8.0 has been rebranded to remove the "Aura" trademark.
Cloud	• Support AEP deployment on AWS Cloud platform • Support AEP deployment on Azure Cloud platform • Support AEP deployment on Google Cloud platform
Operating System	• * AEP 8.1.2 EPM, AUX and MPP OVAs • * AVL 8.4 Support (based on RHEL 8.4) • Enhanced Password requirements on first login • Small Medium and Large profiles supported per OVA • AEP 8.1 Installer for RHEL 8.2+ • EP and MPP now supports user supplied RHEL 7.8+ and RHEL8.2+ • IPv6 is supported for Primary EPM and MPP servers
Nuance Mix / CCAI	• Support for integration of Nuance Mix DLGaaS API
Google Dialogflow/CCAI (Note capacity limitations above)	• * Enhance selection of Dialogflow v3 Projects and Agents • * Provide enhanced Sample App for Voice, Mobile Chat and SMS with AI vendors • * Default Dialogflow VXML should use the StreamingAnalyzeContent method for events • Allow partial responses via streaming API • Licensing distribution to align with ASR model • GoogleDialogflow configurable VAD • Increased performance to support from 450 to 1500 ports per MPP • Improved Dialogflow Config Screens in AEP • Improved AEP/Google Dialogflow Documentation • Improved license management • Enhanced alarm management • Improved Sample Application documentation • Inclusion of VAD package in the Tuning Service • Support for Dialogflow CX • Enhanced reports, intent trends. • Updated (VAD)Voice Activity Detector algorithm, which must be enabled. • Ability to configure Google Dialogflow as an ASR Speech Server. • Support for connectivity to Dialogflow via gRPC • New AAEP License for Google Dialogflow connections • Reporting support for Dialogflow • Supports updating the Google credential dynamically • Per application Google Dialogflow credentials • Embedded default VXML application to simplify Dialogflow integration

Enhancements	Description
	• Supports Dialogflow long running operations • Multi-language support, can be configured via the Dialogflow bot or EP application • Interleaving pre-recorded prompts with Text to Speech • Integrated DTMF detection and handling • Privacy enhancements to include calls to Dialogflow • Support for CX partial responses

Security	• * Local WebLM 8.1 now utilizing AEP Certificate Architecture
	• * Primary EPM linux crypto policy changed from LEGACY -> DEFAULT. Note: Auxiliary and MPP were already at DEFAULT in previous releases
	• Default umask of 027 supported
	• Upload identity certificates for EPM and MPP through the EPM web interface
	• Removal of weak ciphers (AEP 8.0 PSN)
	• SE Linux support (Enforced Mode)
	• Default umask of 022 supported
	• Password complexity enhancements
	• Introduction of a file integrity checker
	• Networking parameters default configuration
	• FIPS Support
	  ○ Voice
	  ○ SIP (SRTP), H323
	  ○ SMS, Email
	  ○ LDAPS
	  ○ AOD
	• Enabling FIPS 140-2 at the OS level also enables FIPS for Java modules. Applies to both the EPM and MPP
	• FIPS 140-2 can now be configured on the underlying RHEL OS
	• Improved protection for database passwords
	• URL Query-strings are no longer logged
	• AAEP enables the ability to use certificate-based authentication for the VPAppLogClient
	• Security Certificate Re-Architecture
	  ○ Reduction from two Identity certificates to one per server.
	  ○ Automatic trust relationship for certificates across servers.
	  ○ Support for importation of chained certificates
	  ○ New Platform certificate type for trust relationships.
	  ○ Limit the number of Root generations without restarting the Primary EPM
	  ○ EPM and MPP Servers Config changes to “Restart Needed”
	• Certificate Revocation List Support
	  ○ Import/Upload of CRLs
	  ○ Validation of certificates against imported/uploaded CRLs.
	• Certificate Expiration Checking

Enhancements	Description
	• Secure connections Syslog Server supported • Security – Concurrent session limiting system wide users' sessions and individual user sessions. • Output from scheduled reports stored in encrypted files • *Axis1 Web Service container is no longer installed*
POM	• * POM 4.0.2 is the minimum version supported in 8.1.2. • POM 4.0.1 Patch 2 is the minimum version supported in 8.1.1. • Outbound performance enhancement with MPP to cache ccxml content • Scheduled reports for POM can be executed in 15- and 30-minute intervals
Licensing	• Enhance vendor-specific speech license distribution to skip a zone that does not have any speech servers that use that license • Latest Avaya legal notice for EPM • Experience Portal now require licenses with version 8. Licenses with version 7 will no longer work. • ASR and TTS licenses are now counted. ***Note**: Do not share Master/Central WebLM between EP 7.x and EP 8.0 systems.*

General	• Capability to modify LDAP Session configuration via webservice
	• Avaya AVA no longer supported
	• Main EPM Tomcat JVM memory allocation increased to 2GB
	• Active Calls Refresh button
	• Additional browser support
	  ○ Chrome 80
	  ○ Edge 44.1763
	  ○ Firefox 74
	  ○ IE 11.1098
	  ○ Safari 10.11
	• Request-URIs can be prioritized over "to" headers

SMS	• Add support for passing Emoji characters to OD SMS apps • Send lengthy SMS as single message with Avaya Zang • Support the ability to share the same Zang account across multiple EP systems • Support for two-way MMS with Avaya Zang connections. • Support i2SMS for outbound SMS. • Support SMPP connections over TLS 1.2.
Reporting	• Speech Usage Metering reporting enhancements • On-demand and schedule reports now generate ".XLXS" output instead of ".XLS" • Intent/Utterance Summary reports with trending for Dialogflow apps • Offer a usage-based license, billed on per minute of usage basis, for each day of the month. • Schedule hourly reports to start running 30 minutes after the hour (to include calls that start before the end of the hour but do not finish)
Speech	• [GRP3BU-5609] AAEP - Create a new CCXML Event to prevent abrupt call termination

Enhancements	Description
	• Support for Third Party ASR & TTS • 1500 concurrent inbound sessions now supported per MPP • Nuance Recognizer 11 (ASR) for Conversational Speech using Dragon Voice add-on • Vocalizer 7 (TTS) • Native Google Speech support for speech to text • Acquire and release speech resources at will • Use multiple speech resources during the same call • Ability to send speech vendor specific parameters • Number of speech enhancements • Enable Speech Server utterance recording
Early media support	• Support the ability for administrators to configure the early media though the EPM web-interface per application.
RFC 4240	• Implement RFC 4240, Basic Network Media Services with SIP.
Codecs support	• Offer the supported codecs, such as G.711 and G.729 in a priority order that is configurable by administrators when sending a SIP INVITE. • Accept the supported codec, such as G.711 and G.729 based on a priority order that is configurable by administrators while receiving a SIP INVITE. • Prioritization of G.711 a-law audio codec while sending audio to external speech servers.
Security Improvements	• Guidelines on how to use Experience Portal in a GDPR environment • Support for administrators to generate a certificate signing request (CSR) that once signed by a third-party Certificate Authority used as the root certificate of the Primary EPM. • Support for administrators to download CSR. • Support for administrators to upload signed certificate that is based on the CSR generated by the system. • Support for the EPM web interface to provide certificate-based authentication as an alternative to requiring the user to enter a user name and password. • Support for EPM Web Services to provide certificate-based authentication as an alternative to requiring the web service client application to specify a user name and password. • TLS 1.2 (only) support for the Avaya Experience Portal system to address security vulnerabilities in prior TLS versions. • $AVAYA_HOME/Support/Security-Tools – New folder for certificate scripts and EASG related scripts. • Due to security concerns, EPM no longer lists the Axis2 web services the product supports on the Axis2 list services web page.
Currency Updates	• * Extensive currency updates as per Trial KT • Apache Tomcat 8.5.72 • PostgreSQL 12.8 • VMWare ESXi 7.0 • JDBC PostgreSQL Driver 42.2.18 • Axis2 1.7.9

Enhancements	Description
	• Java Mail 1.6.2 • JDBC PostgreSQL Driver 42.2.10 (AEP 8.0) • Commons Collections 3.2.2 • Commons Logging 1.2 • Commons Http Client 3.1 • Apache HTTPD 2.4.6-93 (RH 7) • Jasper Reports 6.6.0 • Axis1 dropped
Interoperation	• Aura 10.1 • ASBCE 10.1 • AAOD 7.x app support on AEP 8.0 • CM 8.1.2 support • Aura 8.0, 8.0.1 support, See EXPPORTAL-2723 For limitations.
Platform	• Avaya Common Server (ACP) 110 and 130 support
EASG	• Add capability to enable/disable SSH service for EASG CLI login on AEP running on ASP 130 R5 • EASG fully supported • Minor alarms are generated to flag EASG certificate expiration. • Enhanced Access Security Gateway (EASG) EASG provides a secure method for Avaya services personnel to access the Avaya Experience Portal remotely and onsite. Access is under the control of the customer and can be enabled or disable at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Health check. • EASG Avaya Service Login names are limited to, init, inads, craft, and sroot.
Server Identity Validation	• Support for validating the server certificate identity. • The default setting for Server Identity Validation is o Enabled for freshly installed systems o Disabled for upgraded systems to avoid service disruption. • Attributes required to be supported by External server certificates o Valid Subject Common Name that represents the external server fully qualified hostname o The X509 V3 Subject Alternate Name (SAN) extension should include valid DNS and IP Address entries associated with the external server domain name and actual IP address Note: • For Speech server, SIP Proxy server, and Application server, the SAN extension with both valid DNS and IP Address entries are required to pass the Server Identity Validation. • The DNS entry in the Subject Alternate Name extension can contain the wildcard * (asterisk) character which can match any single domain name component or component fragment. For example, *.avaya.com matches ep.avaya.com, but it does not match bar.ep.avaya.com. e*.com matches ep.com but it does not match bar.com.

Enhancements	Description
	• Wildcard in DNS entry is not valid for SIP server.

For detailed descriptions of the enhancements in this release see ***Avaya Experience Portal Overview and Specification*** *(*https://downloads.avaya.com/css/P8/documents/101083227*)*.

Additional Information for New Features Delivered in AEP 8.1+

Upload of Identity Certificates for EPM and MPP through the EP admin web interface

AEP 8.1+ supports upload and installation of custom identity certificates (PKI) for EPM and MPP servers through the EP web admin interface.

The upload functionality is available by navigating to;

- Certificates > Security > EPM Identity Certificates tab or
- Certificates > Security > MPP Identity Certificates tab

Refer to the Certificates chapter of the Administering Experience Portal documentation for relevant procedures.

These new procedures replace the use of the SetupServerCertificate.sh -import script to install custom identity certificates for EP servers.

SELinux in Enforcing mode

AEP 8.1+ now fully supports SELinux in enforcing mode.

AEP 8.1.2 OVAs

- Three OVAs are provided:
  - ExperiencePortal-Primary-EPM
  - ExperiencePortal-Auxiliary-EPM
  - ExperiencePortal-MPP
- Deploy OVAs using VMware vSphere
- AEP OVAs fail to deploy on older versions of VMWare ESXi. Make sure your ESXi is updated to the latest VMWare release. AEP has been verified on the following ESXi versions:
  - ESXi 6.5 P04 *
  - ESXi 6.7 P01 *
  - ESXi 7.0 Update 2a
  - * As of October 15, 2022, VMWare is Ending General Support for vSphere 6.5 and vSphere 6.7
- No current OVA limitations
- MPP and EPM profiles are as follows:

MPP Profiles	
Profile Label	**Resources**
Entry	4 CPUs + 4GB RAM
Small	8 CPUs + 8GB RAM
Medium / Typical	8 CPUs + 16GB RAM
Large	12 CPUs + 24GB RAM

EPM Profile	
Profile Label	**Resources**
Entry	2 CPUs + 4GB RAM
Standard / Typical	6 CPUs + 12GB RAM

Deploying OVAs

Once the OVA is deployed on VMWare and the user starts up the virtual server. The first boot can take up to 12 minutes for Primary and Auxiliary EPM and five minutes for MPP.

CAVEAT: Make sure the Primary EPM is up and running and you can logon to ssh session before the Auxiliary EPM or MPP is started.

Once the OVAs are up and running logon to ssh session (either using VMWare console or putty into the IP address entered during installation).and do the following:

1. Start Primary EPM OVA first.
2. Start putty session to Primary EPM IP address and logon as **cust** / **custpw**

NOTE: There is a “Password expired” “

3. Run command **su -**
4. Password: **rootpw**
5. You will then be asked to change bootloader, root, and cust passwords

FIPS 140-2 Support

- **Enabling** FIPS Mode on **RHEL7** system
  - RedHat publish instructions on how to enable FIPS Mode in RedHat 7: Enable FIPS Mode RHEL7
  - Follow these instructions and then run command to verify that FIPS is enabled: *sysctl crypto.fips_enabled*
  - A reboot is required after FIPS is enabled.
- **Disabling** FIPS Mode on **RHEL7** system
  - Follow RedHat instructions on disabling FIPS and reboot the system.
  - Run command:

    bash /opt/Avaya/ExperiencePortal/Support/Security-Tools/AAEP_FIPS_remove.sh
  - Reboot.
- **Enabling** FIPS Mode on **AVL** or **OVA** or **RHEL8** system
  - RHEL8 has introduced a new easy method of enabling / disabling FIPS using command: fips-mode-setup
  - To enable FIPS on AVL or OVA or RHEL8:
    1. Run command: fips-mode-setup --enable
    2. Reboot
- **Disabling** FIPS Mode on **AVL** or **OVA** or **RHEL8** system
  - RHEL8 has introduced a new easy method of enabling / disabling FIPS using command: fips-mode-setup
  - To disable FIPS on AVL or OVA or RHEL8:
    1. Run the commands

       fips-mode-setup –disable

       reboot

       bash /opt/Avaya/ExperiencePortal/Support/Security-Tools/AAEP_FIPS_remove.sh
    2. Reboot

Microsoft SQL Server external database connections with FIPS

A new database truststore is required for SQL Server connections with FIPS. Follow these steps to create and configure the truststore:

1. Import the SQL server certificate(s) to a database truststore on the Primary EPM using the command

   keytool -keystore <dbtruststorename.bks> -import -alias <aliasname> -file <certificate> -noprompt -storepass <storepass> -storetype BCFKS -providerpath $JAVA_HOME/jre/lib/ext/bc-fips-1.0.1.jar -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider

Example:

keytool -keystore database.bks -import -alias sqlserver1 -file server1.cer -noprompt -storepass changeit -storetype BCFKS -providerpath $JAVA_HOME/jre/lib/ext/bc-fips-1.0.1.jar -provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider

2. Configure the database connection URL under EPM screen "EPM Servers > Data Storage Settings" using the format:

   jdbc:sqlserver://<sqlserver-hostaddress>:1433;databaseName=<databasename>;TrustServerCertificate=false;encrypt=true;fips=true;fipsProvider=BCFIPS;trustStoreType=BCFKS;trustStore=<fully qualified path to the database truststore>;trustStorePassword=<trustStorePassword>

   Example:

   jdbc:sqlserver://server1.avaya.com:1433;databaseName=EP;TrustServerCertificate=false;encrypt=true;fips=true;fipsProvider=BCFIPS;trustStoreType=BCFKS;trustStore=/opt/Tomcat/tomcat/conf/database.bks;trustStorePassword=changeit

Known Issues

1. Install/Reinstall will not work with FIPS enabled.

   Workaround: Disable FIPS before running any fresh installs or upgrades.

Upgrading the RHEL 7.8 or RHEL 8.2+ or AVL 8.2 based EPM, Aux EPM and MPP

Introduced in AEP 8.1+ is the ability to upgrade from AEP 6.x or 7.x using either Avaya Enterprise Linux or RHEL 7.8+ / 8.2+. The key points relating to upgrading to AEP 8.1.2 are as follows:

- Supported upgrade paths:
  - AVL based EP deployments
    - EP 6.x/7.x -> EP 8.1.2, upgrade AVL to RHEL 8, then install EP using product ISO
    - EP 8.x -> EP 8.1.2 upgrades using product ISO after applying latest AVL security Patch.
      - AVL 8.x cannot be upgraded, applying the latest AVL security patch will provide the same functionality.
      - For example, upgrading AVL 8.1 AVL 8.1 AvayaLinux-RH8.2.64-AV18EP8.26May21.112601 to AVL 8.1.2 AvayaLinux-RH8.4.64-AV04EP8.27Jun22.132645.iso is not supported
      - Use the upgrade option during AVL patch install, this will apply all needed changes to support the product on the original AVL.
        - ./setup.sh -v 8.1.2
      - Then the product can be upgraded.
  - RHEL based EP deployments
    - EP 6.x/7.x -> EP 8.1.2 migration
    - EP 8.x -> EP 8.1.2 upgrade
  - OVA based deployments
    - EP 8.0 OVAs -> EP 8.1.2 upgrades using product ISO after applying latest AVL security Patch.
      - AVL 8.x cannot be upgraded, applying the latest AVL security patch will provide the same functionality.
      - For example, upgrading AVL 8.1 AVL 8.1 AvayaLinux-RH8.2.64-AV18EP8.26May21.112601 to AVL 8.1.2 AvayaLinux-RH8.4.64-AV04EP8.27Jun22.132645.iso is not supported

        - Use the upgrade option during AVL patch install, this will apply all needed changes to support the product on the original AVL.
            - ./setup.sh -v 8.1.2
        - Then the product can be upgraded.
    - In-place OVA upgrades from EP 6.x/7.x are not supported to 8.1.2
        - EP 8.1.2 OVA(s) must be deployed
- Upgrading from RHEL EP 6.x/7.x to EP 8.1.2 requires manual backup and staging of database and configuration files onto the Primary EPM
- If custom certificates are configured in the solution:
    - Ensure the Certificate Authority (CA) trusted certificate is available
    - Ensure the required PKCS#12 (.p12) files for each server are available and ready for import into their respective servers
    - Ensure that the password for the supplied .p12 files are known as they will be required when importing in the files into AAEP
- The complete upgrade procedure, including prerequisites and step-by-step instructions, is detailed in the ***Upgrading to Avaya Experience Portal 8.1*** *(*https://downloads.avaya.com/css/P8/documents/101083233*)* document**.**

Fixes

The following table is cumulative since the release of AEP 8.0 showing the most recent release first and oldest release last. This table is currently empty and will be populated with fixes delivered in potential Post GA patches or subsequent Service Packs or Feature Packs.

All fixes delivered in Experience Portal 8.0 and 8.1 are included in Experience Portal 8.1.2

ID	Minimum Conditions	Visible symptoms	Release found in	Release fixed in

Known issues and workarounds

Installation Issues

ID	Minimum conditions	Visible symptoms	Workaround
NA	Upgrading a system that uses an external reporting database	No new data appears in the Session Detail or Session Summary report.	The appropriate database script referenced in help topic '*Updating the external database configuration*' should ideally be run prior to upgrading EPM software to version 8.1. However, the script can also be run after an upgrade to restore the proper insertion of data to the database. The .sql files are in the directory /Support/ExternalDB/<DBVENDOR>/UpgradeScripts. Where, <DBVENDOR> can be Oracle, Postgres, MSSQL, or MySQL. If you use Oracle: For an 8.0 to 8.1 upgrade scenario, run the Oracle_New_Columns_81.sql script. If you use Postgres: For an 8.0 to 8.1 upgrade scenario, run the New_Columns_81.sql script. If you use Microsoft SQLServer: For an 8.0 to 8.1 upgrade scenario, run the MSSQL_New_Columns_81.sql script. If you use MySQL or MariaDb: For an 8.0 to 8.1 upgrade scenario, run the MySQL_New_Columns_81.sql script.

N/A	Installing or Upgrading Experience Portal Primary or Auxiliary EPM	TLS communications fail with errors like "invalid protocol version" or "protocol_error"	Ensure that the surrounding environment including external servers uses TLS 1.2 protocols for establishing secure communications with Experience Portal.
			
			Suggestions
			External Servers (excluding Enterprise WebLM Servers)
			Here are some suggestions for updating external servers using older versions of Oracle JDK. If the server is using a different flavor of JDK, then install the latest version of that flavor which supports TLS 1.2 by default.
			• **Java based servers** (Application servers including servers hosting Redirector application)
			  • Servers using Oracle JDK 1.6.0 must use Oracle JDK 1.6.0 Update 141 or later.
			  • Servers using Oracle JDK 1.7.0 must use Oracle JDK 1.7.0 Update 131 or later.
			  • Server using Oracle JDK 1.8.0 or higher, no change is required.
			
			Enterprise WebLM Server
			Enterprise WebLM server which is using an older version of JDK will not be able to allocate licenses to

ID	Minimum conditions	Visible symptoms	Workaround
			the Local WebLM Server on the Primary EPM using TLS 1.2. To continue using Enterprise Licensing with TLS 1.2, it is required that Enterprise WebLM Server is upgraded to the 7.0.1 version which supports/includes JDK 1.8.0. If an Enterprise WebLM Server is not available for the environment being used, then enable TLS 1.0 and TLS 1.1 for port 8443, using the following steps on the Primary EPM: 1. Take a backup of the file /etc/httpd/conf.d/vpms.conf 2. Edit the /etc/httpd/conf.d/vpms.conf file and perform the following steps: a. Remove -TLSv1 -TLSv1.1 from the SSLProtocol line shown in the section shown below: b. Replace the SSLCipherSuite line with SSLCipherSuite HIGH:MEDIUM:!ADH:!EDH:!RC4:!MD5:!3DES:!IDEA <VirtualHost _default_:8443> ServerAlias * RewriteEngine On RewriteOptions Inherit RewriteRule ^/(VoicePortal(/(.*))?)?$ https://%{SERVER_NAME}/VoicePortal/$3 [R=301,L] SSLEngine on SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 SSLCipherSuite FIPS:!3DES:!ADH:!SHA:!EDH SSLCertificateFile /etc/pki/tls/certs/weblmserver.crt SSLCertificateKeyFile /etc/pki/tls/private/weblmserver.key ProxyPass /WebLM ajp://localhost:3009/WebLM </VirtualHost> 3. Restart the Apache service using the command “/sbin/service httpd restart”. **Note**: If the system is reinstalled or upgraded to a newer version, these steps need to be re-applied. **Note**: If the external servers cannot be updated to using TLS 1.2, then during the transition period, the TLS 1.0 and TLS 1.1 protocols can be enabled on the EP servers using the script $AVAYA_HOME/Support/Security-Tools/ConfigureLegacyTLS.sh. It is highly recommended that once the external servers are updated to use TLS 1.2, the TLS 1.0 and TLS 1.1 protocols are disabled on all the EP servers using the same script.
N/A	Installing or Upgrading Experience Portal Primary EPM in a	Local WebLM server does not show any Server Host ID under Server Properties web page.	To work around this issue, add the local hostname/IP to the /etc/hosts file even though the hostname/IP address is also in the DNS.

ID	Minimum conditions	Visible symptoms	Workaround
	network environment with DNS and co-residing WebLM server is used for hosting either Enterprise or Allocation licenses.	As WebLM server does not have a Server Host ID, installation of a license file fails.	
N/A	Upgrading Experience Portal Primary or Auxiliary EPM Upgrading from releases prior to Experience Portal 7.0.x	Outcalls fail during upgrade if EPM name contains space. Applications can make outcalls using the Application Interface web service. This web service runs on the Primary EPM server and on all Auxiliary EPM servers. Normally, throughout the upgrade process at least once instance of the Application Interface web service is available to make outcalls. However, if the name of the Primary EPM or any Auxiliary EPM contains a space (" ") character, then there may be a period of several minutes during the upgrade when all instances of the Application Interface web service are out of service at the same time. Note that once the upgrade is completed, all instances of the Application Interface web service will again operate correctly.	To work around this issue, remove all space characters from your EPM names before starting the upgrade.
NA	Sites using SMS or Email processors on the EPM	CDR records from OD SMS or email applications not shown in the Contact Summary or Contact Detail reports	During the Postgres 11 upgrade, the sequence counter columns are impacted due to the need for a database restore. The restore sets the auto incremented counter value to 0 and that interferes with the scheme used to detect and download "new" CDR and SDR from the Multimedia database to the reporting database. Sites using Email and/or SMS processors on the EPM need to refer to EPM help topic "**Ensuring new SMS and Email records are created after upgrades**."
EXPPORTAL-3645	IPv6 environment	AEP 8.0 - IPv6 license server does not connect	• Install the Experience Portal license on the WebLM server that co-resides with the Primary EPM and access that server using the IPv4 loopback address (127.0.0.1) or

ID	Minimum conditions	Visible symptoms	Workaround
			• Install the Experience Portal license on an external WebLM server that is accessible via IPv4
EXPPORTAL-3556		AAEP can't establish the connection to SMPP in IPv6 mode	Use IPv4 for SMPP
EXPPORTAL-3552		AAEP can't pass the full grammar from VXML application which is deployed external app server (Ipv6) to Nuance	Use an IPv4 Application server address.
EXPPORTAL-3551		The Data Storage Settings does not save and return error message when using IPv6 address decorated with square brackets (SQL Server)	Refer to Microsoft SQL Server documentation for the IPv6 address format when specifying the SQL Server host address
SMGR-54468		Cannot use FIPS SMGR as a CA	1. Add EPM as an End Entity on SMGR Security with Token Type = JKS. 2. Create Keystore and download the JKS certificate. 3. Cope the JKS certificate to the EPM server and run the Keytool command to convert the JKS certificate to a p12 certificate. 4. Convert the JKS to p.12: keytool -importkeystore -srckeystore <end_entity_name>.jks -destkeystore pkcs_filename.p12 -srcalias <end_entity_name> -srcstoretype JKS -deststoretype PKCS12 -deststorepass <PKCS12_password> -srcstorepass <end_entity_password> 5. Use the SetupServerCertificate.sh -import command and follow steps to install custom p12 certificate.
EXPPORTAL-7029	OVAs: Alarm report displays both EPM and MPP alarms when only EPM server selected	Alarm report displays both EPM and MPP alarms when only EPM server selected	This is caused by the /etc/hosts file not containing the short hostname for all servers. Edit the /etc/hosts file to include short hostname for all servers: e.g. 192.168.1.5 pri-epm-5.example.com pri-epm-5
EXPPORTAL-8819	Cannot migrate EPM from 7.1 to 8.1.2	Migration from AAEP 7.1 to AEP 8.1.2 fails for vpupgrade.sh *ERROR: Errors encountered while running schemaUpgrade.sh script.*	
N/A	Applications may have to be reworked to be more standards compliant	MozJS interpreters have been upgraded (mozjs52) and are more standards/syntax compliant. This may reject code that was previously allowed.	Rework applications to be more standards compliant.

ID	Minimum conditions	Visible symptoms	Workaround
N/A	Upgrading or patching an MPP	The directories for the Default VXML applications for Nuance Mix and Dialogflow under the $MPP/web/misc directory are overwritten	The Default VXML applications (and associated prompts) should not be modified as it will be overwritten during upgrades. If a customer requires customization, then the entire VXML application directory must be copied and changes made to the copied version only. Avaya recommends copying the entire folder (dialogflowapp or nuancemixapp) as the entire folders are over-written during upgrades (all customer created files are deleted).
N/A	FIPS: Tomcat does not start in a FIPS enabled customer supplied RedHat linux server	catalina.log shows the following exception: `java.security.ProviderException: Crypto provider not installed: BCFIPS SunPKCS11-NSS-FIPS`	Resolution: Set up RHEL yum repo and run command: yum update –y
EXPPORTAL-9866	Cannot upload/import certificates via REST web services	The EPWebServices REST APIs for trusted certificate upload and import return 404 Not Found	Upload/import trusted certificates through the EP Web interface EP Web Admin -> Security -> Certificates

Avaya Linux 8 Issues

ID	Minimum conditions	Visible symptoms	Workaround
N/A	Using the “Red Hat Enterprise Linux 8 (64-bit)” template in VMware 6,7 and 7.0	Cannot boot from ISO, will display “EFI ???… Unsuccessful	In the VM Options -> Boot Options change the Firmware from EFI to BIOS
EXPPORTAL-5186	Setting password on first root login	System enforces password complexity with pwscore.	Use a more complex password

Avaya Orchestration Designer Issues

ID	Minimum conditions	Visible symptoms	Workaround

System Operation Issues

ID	Minimum conditions	Visible symptoms	Workaround
PSN003432u		Time not displayed correctly for a time zone. Typically, Experience Portal displays times in either the local time of the Primary EPM server or in the local	To fix time zone related display issues, update each Experience Portal server to the latest version of the Linux time zone information RPM, tzdata. Also update the time zone information used by the Java

ID	Minimum conditions	Visible symptoms	Workaround
		time of the user's web browser. Sometimes the time displayed by Experience Portal is not correct for a particular time zone because the rules for that time zone have changed recently. In a typical year, for example, there are several countries around the world that either adopt or abandon daylight saving time (also known as summer time), or adjust when daylight saving time begins or ends.	Runtime Environment (JRE) on each Primary EPM and each Auxiliary EPM server. See PSN003432u (http://downloads.avaya.com/css/P8/documents/100149873) for the procedure details.
EXPPORTAL-295	MPP name contains hash character and attempting to view transcript data.	Cannot view transcriptions if MPP name contains hash. The **Session Detail Report** can optionally display a transcription that shows the details of what happened during a session. For example, the session transcription will show all VoiceXML pages loaded, all prompts played, and all utterances spoken by the caller. The **Session Detail Report**, however, will fail to show the session transcription if the name of the MPP that processed the call contains a hash ("#") character.	To work around this issue, remove all hash characters from your MPP names. Note that the **Change MPP Server** web page does not allow you to edit the name of an MPP. You must delete and re-add any MPP whose name you wish to change.
EXPPORTAL-846	Deleting and re-adding Aux EPM servers with the same name but different IP addresses	This doubles the number of HTML licenses used by that server. This can cause HTML license capacity to expire prematurely.	The problem automatically fixes itself when HTML licenses reset at the end of each day.
EXPPORTAL-894	EP Application Interface web service and .NET	Cannot generate web service client proxy using WSDL for .NET	Contact Avaya Support.
EXPPORTAL-1518	Upgrade OS after EP 7.2 install.	If the current EASG state is enabled of an EP 7.2 server, the EASG might not be protected (no challenge/response prompt for Avaya service accounts login) after subsequent OS upgrade and EP 7.2 upgrade.	Toggle the EASG state by running the following two commands on the EP 7.2 server: #1, “bash $AVAYA_HOME/Support/Security-Tools/EASG/EASGConfigure.sh --disable” #2, “bash $AVAYA_HOME/Support/Security-Tools/EASG/EASGConfigure.sh --enable”
EXPPORTAL-3358	Using Google Dialogflow	Google do not guarantee response times to method calls and state that the majority of calls will complete in a short period of time, but a small fraction of a percentage will take longer than 1 second.	AEP sets an 8 second deadline on method calls to Google Dialogflow, if exceeded will throw a speech error. Applications must catch this error and handle - retry to set up the session to Google or default to an alternative speech vendor.

ID	Minimum conditions	Visible symptoms	Workaround
EXPPORTAL-6801	At least one email or SMS connection is configured.	EPM System Monitor indicates the Email or SMS processor is in a Stopped state.	Issue the command "*systemctl enable mmsserver*" in a console window on the EPM and Aux EPM and start the mmsserver service using "*systemctl start mmsserver"* command.
EXPPORTAL-9867	EP application utilizing the VXML <data/> tag	Execution of <data> tag generates a PAVB_03049 ECMA script error exception. Description = Unspecified script error occurred.	Contact Avaya Support.

Languages supported

Region	Country	Written Language
APAC		
	Australia	English
	China	Simplified Chinese
	India	English
	Japan	Japanese
	Korea	Korean
EMEA		
	France	French
	Germany	German
	Italy	Italian
	Russia	Russian
	UK	English
AI		
	Brazil	Brazilian-Portuguese
	Canada	French/English
	Mexico	Lat-Spanish
US		
	US	English

Contacting support

Contact Support Checklist

Refer to the Troubleshooting section in the Avaya Experience Portal 8.0 Documentation Library. Or refer to the ***Troubleshooting Avaya Experience Portal*** document on the Avaya Technical Support web site https://support.avaya.com.

If you are having trouble with Avaya Experience Portal, you should:

1. Retry the action. Carefully follow the instructions in written or online documentation.
2. Check the documentation that came with your hardware for maintenance or hardware-related problems.
3. 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.