



Avaya Experience Portal 8.0 Release Notes

Release 8.0
Issue 1.7
April 2021

© 2021, Avaya Inc.
All Rights Reserved.

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](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	1
Introduction	1
Installation	1
Installing the release.....	1
Troubleshooting the installation.....	3
Product compatibility.....	3
File list.....	4
Backing up the software.....	6
Functionality not supported	6
Google Dialogflow Issue: Dialogflow connectivity slow detection of dead TCP connections	6
What's new	7
Additional Information for New Features Delivered in AEP 8.0	11
AEP 8.0 Installation.....	11
AEP 8.0 OVAs	11
Deploying OVAs	11
FIPS 140-2 Support	11
Microsoft SQL Server external database connections with FIPS	12
Known Issues	12
Upgrading the RHEL 7.8 or RHEL 8.2 or AVL 8.2 based EPM, Aux EPM and MPP	13
Fixes	14
Known issues and workarounds	14
Installation Issues	16
Avaya Linux 8.2 Issues	21
System Operation Issues	21
Languages supported	23
Contacting support	23
Contact Support Checklist	23
Contact Support Tasks	23

Document changes

Issue	Date	Description
1.0	29 September 2020	GA version for AEP 8.0
1.1	13 October 2020	Document removal of Axis2 list Services.
1.2	16 October 2020	AVL must use BIOS boot
1.3	2 November 2020	GA update version for AEP 8.0 to replace MySQL connector with MariaDB connector and deliver additional bugfix. All deployment images have been up-issued and supersede the original images released on 29-Sep.
1.4	9 November 2020	Updated with comments from the Avaya DevConnect team.
1.5	22 December 2020	Update to align with Patch 8.0.0.0.1424 and POM 4.0 GA.
1.6	18 January 2021	Update for revised Aux OVA (1217-1)
1.7	26 April 2021	Update to align with Patch 8.0.0.0.1451

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>.

Installation

Installing the release

AEP 8.0 introduces a new installer mechanism. This section covers this new procedure.

Note: This section covers both fresh installation of AEP 8.0 and upgrades from a previous version of AEP 8.0 that was released (8.0.0.0.0498).

General Notes

- RHEL 7.8 and 8.2 version supported as well as AVL (based on RHEL 8.2)
- Customer must 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)
- SELinux must be set to disabled or permissive. SELinux enforcing is not supported. Installer will abort if detected.
- Linux umask value with the world-readable bit set to zero MUST be configured: i.e. Octal: xxx xxx 0xx (i.e. 022)
- 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 needs to be disabled (Installer will disable firewall if enabled)
- EPM must have chronyd (NTP) configured.

Fresh RPM Install instructions

1. Install RHEL 7.8 or RHEL 8.2 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 EPM
5. Set selinux to either "permissive" or "disabled" in file `/etc/selinux/config`. A reboot is required after changing selinux.
6. Set up yum repo from 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\nngpgcheck=0" >>
/etc/yum.repos.d/media.repo

RHEL8: echo -e "baseurl=file:///mnt/cdrom/BaseOS\nenabled=1\nngpgcheck=0\n[InstallMedia-AppStream]\nname=Red Hat Enterprise Linux 8 - AppStream\nmetadata_expire=-1\nenabled=1\nbaseurl=file:///mnt/cdrom/AppStream/\nngpgcheck=0\n" >>
/etc/yum.repos.d/media.repo
```
7. Mount the **AEP-8.0.0.0.1217.iso** file on Linux server.

One method to do this is:

 - i. Copy AEP-8.0.0.0.1217.iso file to /tmp folder on Linux server
 - ii. Run command: `mkdir -p /mnt/aep80`
 - iii. Run command: `mount -o loop AEP-8.0.0.0.1217.iso /mnt/aep80`
8. Run the following command to install EPM or MPP:
 - i. `cd /mnt/aep80`
 - ii. `bash aaepinstall.sh`
9. Select option to install either:
 - i. Primary EPM
 - ii. Auxiliary EPM
 - iii. Standalone MPP
 - iv. Single Server - Primary EPM and MPP
10. Install time of EPM is approximately 20 minutes. MPP Install time is approximately 5 minutes.
11. If FIPS is required, then enable FIPS as per [FIPS 140-2 Support](#)
12. For EPM: Logon to Web admin using: https://<EPM_IP>/VoicePortal with Web admin user and password entered during installation

Upgrading from 8.0.0.0.0498

Note: This procedure is used for upgrading both OVA upgrades and regular AEP upgrades.

Note: To continue to receive product security and bug fix patches it is mandatory to move to the 8.0.0.0.1217 release. All future 8.0.0 patches will not install on any system that is not on the 8.0.0.0.1217 base.

The `aaepinstall.sh` supports in-place upgrades from the previous version of AEP 8.0 released: 8.0.0.0.0498. As this is an upgrade all the pre-requisites should already be applied.

1. Mount the **AEP-8.0.0.0.1217.iso** file on Linux server.

One method to do this is:

- i. Copy AEP-8.0.0.0.1217.iso file to /tmp folder on Linux server
 - ii. Run command: mkdir -p /mnt/aep80
 - iii. Run command: mount -o loop AEP-8.0.0.0.1217.iso /mnt/aep80
2. Run the following commands to upgrade the AEP server:
- i. cd /mnt/aep80
 - ii. bash aaepinstall.sh

aaepinstall.sh will upgrade the AEP 8.0 server to version: 8.0.0.0.1217

Upgrade time of EPM is approximately 20 minutes. MPP upgrade time is approximately 5 minutes.

3. For EPM: Logon to Web admin using: https://<EPM_IP>/VoicePortal with Web admin user and password entered during installation

Known Issues

1. Install will not work 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/101069324>) or **Implementing Avaya Experience Portal on a single server** (<https://downloads.avaya.com/css/P8/documents/101069322>). For upgrades see the document **Upgrading to Avaya Experience Portal 8.0** (<https://downloads.avaya.com/css/P8/documents/101070956>).

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/101069332>).

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://downloads.avaya.com/css/P8/documents/101069318>).

Product compatibility

Note the following limitations.

Application	Compatibility Description	Recommendation
Proactive Outreach Manager (POM)	Due to the OS upgrade in AEP 8.0, POM 4.0 is required as well as a minimum of the 8.0.0.0.1424 patch installed.	Verify compatibility from the matrix referenced below
Intelligent Call Routing (ICR)	Due to the OS upgrade in AEP 8.0, ICR currently is not supported until a compatible ICR release is available.	Verify compatibility from the matrix referenced below
all Back Assist (CBA)	Due to the OS upgrade in AEP 8.0, CBA currently is not supported until a compatible CBA release is available.	Verify compatibility from the matrix referenced below
Dynamic Self Service (DSS)	Due to the OS upgrade in AEP 8.0, DSS currently is not supported until a compatible DSS release is available.	Verify compatibility from the matrix referenced below

--	--	--

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 8.0 software using SHA256 Checksum

All Avaya Experience Portal 8.0 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-8.0.0.0.1217.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 8.0 software

Filename	SHA256 Checksum	File size	Version number
AEP-8.0.0.0.1217.iso	40fe4659e4d9147460ad3768044acf9cb655762c24c25d01cc4d856ddb2c0a12	2,372,634,624	8.0.0.0-1217
AEP-8.0.0.0.1217.sha256.sig	749db9b4d316cd9b9c89211bff5640fa00ecc36ad667f2352797a4879b9953e8	1KB	8.0.0.0-1217
Avaya_Public_Certificate_2023.crt	8d8cbd900e39501c92b9ef180c6a4d9c3653a463e14f5792de43f68ff6aa781f	2K	

File list - Avaya Experience Portal 8.0 OVA software

Filename	SHA256 Checksum	File size	Version number
ExperiencePortal-Primary-EPM-8.0.0.0.1217.ova	4ad4f01949cfa68e445e595b8249834a6f65bfd937f2a04872c1a482f918d14e	5,811,800,064	8.0.0.0-1217
ExperiencePortal-Primary-EPM-8.0.0.0.1217.sha256sum.sig	92afef089305a38bdcc4d0f40699098beeb423dc05f6e27cbab2d1488e1606840	256	8.0.0.0-1217
ExperiencePortal-Auxiliary-EPM-8.0.0.0.1217-1.ova	576d315631e091f758e82002315540fe593aa2672f09de609a3dafbbcf58b54a	5,581,308,928	8.0.0.0-1217
ExperiencePortal-Auxiliary-EPM-8.0.0.0.1217-1.sha256sum.sig	a6ed738d6b28ae90c81288aac641269e06a978cdd77997bd0549ef775714796	256	8.0.0.0-1217
ExperiencePortal-MPP-8.0.0.0.1217.ova	e13b5a7599956fa61594bdc5d6579e455596afe80623f3e72208ecbebb7223f9	5,082,561,536	8.0.0.0-1217
ExperiencePortal-MPP-8.0.0.0.1217.sha256sum.sig	4d6c9a6402afdeefe2ce1b6428cca4602ed0224b98ed28da2bed662701148db2	256	8.0.0.0-1217
Avaya_Public_Certificate_2023.crt	8d8cbd900e39501c92b9ef180c6a4d9c3653a463e14f5792de43f68ff6aa781f	1,777	

File list - Avaya Enterprise Linux for Avaya Experience Portal 8.0 software

Backing up the software

Important: Experience Portal 8.0 introduces a new procedure for upgrading to 8.0 which requires manual backup and restore of configuration data.

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 in order 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 8.0** (<https://downloads.avaya.com/css/P8/documents/101070956>).

Functionality not supported

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

Google Dialogflow capacity is limited to a maximum of 450 concurrent calls active to Dialogflow per MPP. This does not impact any other call or speech vendor capacity.

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.

In order 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.

What's new

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

**New in AEP 8.0*

Enhancements	Description
Branding	<ul style="list-style-type: none"> *Experience Portal has been rebranded to remove the “Aura” trademark.
Operating System	<ul style="list-style-type: none"> * AEP 8.0 EPM, AUX and MPP OVAs *Small Medium and Large profiles supported per OVA *AVL 8.2 Support *AEP 8.0 Installer for RHEL 8.2 *8.0 License – AEP *EP and MPP now supports user supplied RHEL 7 and RHEL8. *IPv6 is supported for Primary EPM and MPP servers
Google Dialogflow/CCAI (Note capacity limitations above)	<ul style="list-style-type: none"> *Support for Dialogflow CX (currently Beta) *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 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
Security	<ul style="list-style-type: none"> *FIPS Support <ul style="list-style-type: none"> o Voice o SIP (SRTP), H323 o SMS, Email o LDAPS o 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 VAppLogClient *Security Certificate Re-Architecture

Enhancements	Description
	<ul style="list-style-type: none"> ○ 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. ● *Certificate Revocation List Support <ul style="list-style-type: none"> ○ Import/Upload of CRLs ○ Validation of certificates against imported/uploaded CRLs. ● *Certificate Expiration Checking ● *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	<ul style="list-style-type: none"> ● *POM is currently not supported in 8.0 until an aligned release of POM (4.0) is available. ● Scheduled reports for POM can be executed in 15- and 30-minute intervals
Licensing	<ul style="list-style-type: none"> ● *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	<ul style="list-style-type: none"> ● *Avaya AVA no longer supported ● *Main EPM Tomcat JVM memory allocation increased to 2GB ● *Active Calls Refresh button ● *Additional browser support <ul style="list-style-type: none"> ○ Chrome 80 ○ Edge 44.1763 ○ Firefox 74 ○ IE 11.1098 ○ Safari 10.11 ● *Request-URIs can be prioritized over “to” headers
SMS	<ul style="list-style-type: none"> ● *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	<ul style="list-style-type: none"> ● *On-demand and schedule reports now generates “.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)

Enhancements	Description
Speech	<ul style="list-style-type: none"> • *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 • Support Nuance Session XML • Enable Speech Server utterance recording • Improved user interface for selecting languages and voices
Early media support	<ul style="list-style-type: none"> • Support the ability for administrators to configure the early media through the EPM web-interface per application.
RFC 4240	<ul style="list-style-type: none"> • Implement RFC 4240, Basic Network Media Services with SIP.
Global CAVs	<ul style="list-style-type: none"> • Ability for administrators to configure the user defined global Configurable Application Variables. These are system wide variables that are not specific to an application.
Codecs support	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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. • Scripts SetupServerCertificate.sh and ImportExternalServerCertificate.sh provide the functionality previously provided by GenerateServerCertificate.sh & ImportServerCertificate.sh. • \$AVAYA_HOME/Support/Security-Tools – New folder for certificate scripts and EASG related scripts.
Currency Updates	<ul style="list-style-type: none"> • *Apache Tomcat 8.5.57 • *Axis2 1.7.9

Enhancements	Description
	<ul style="list-style-type: none"> • *Java Mail 1.6.2 • *JDBC PostgreSQL Drive 42.2.10 • *Commons Collections 3.2.2 • *Commons Logging 1.2 • *Commons Http Client 3.1 • *Apache HTTPD 2.4.6-93 (RH 7) • VMWare ESXi 6.7 • PostgreSQL 11.4 • Jasper Reports 6.6.0 • Axis1 dropped
Interoperation	<ul style="list-style-type: none"> • *AOD 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	<ul style="list-style-type: none"> • Avaya Common Server (ACP) 110 and 130 support
EASG	<ul style="list-style-type: none"> • *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 disabled 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	<ul style="list-style-type: none"> • Support for validating the server certificate identity. • The default setting for Server Identity Validation is <ul style="list-style-type: none"> ○ Enabled for freshly installed systems ○ Disabled for upgraded systems to avoid service disruption. • Attributes required to be supported by External server certificates <ul style="list-style-type: none"> ○ Valid Subject Common Name that represents the external server fully qualified hostname ○ 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 <p>Note:</p> <ul style="list-style-type: none"> • 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. • 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/101069316>).

Additional Information for New Features Delivered in AEP 8.0

AEP 8.0 Installation

AEP 8.0 has introduced a new mechanism of installation. This is covered in section: [Installing the release](#)

AEP 8.0 OVAs

- Three OVAs are provided:
 - ExperiencePortal-Primary-EPM
 - ExperiencePortal-Auxiliary-EPM
 - ExperiencePortal-MPP
- Deploy OVAs using VMware vSphere
- Three deployment footprints/templates:
 - Minimal - 4 CPUs and 4GB Memory
 - Typical - 8 CPUs and 12GB Memory
 - Large - 12 CPUs and 32GB Memory
- No current OVA limitations

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**
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`
 - Java FIPS is automatically configured/enabled when VPMS restarts. A reboot is required after FIPS is enabled.
 - To restart VPMS run command: `systemctl restart vpms`
- Disabling FIPS Mode on RHEL7 system
 - Follow RedHat instructions on disabling FIPS.
 - Run command:
`bash /opt/Avaya/ExperiencePortal/Support/SecurityTools/AAEP_FIPS_remove.sh`
- Enabling FIPS Mode on AVL or RHEL8 system
 - RHEL8 have introduced a new easy method of enabling / disabling FIPS using command: `fips-mode-setup`
 - To Enable FIPS on AVL or RHEL8:

1. Run command: `fips-mode-setup --enable`
 2. Reboot
- Java FIPS is automatically configured/enabled when VPMS restarts. A reboot is required after FIPS is enabled.
 - To restart VPMS run command: `systemctl restart vpms`
- Disabling FIPS Mode on RHEL8 system
 1. Run command: `fips-mode-setup --disable`
 2. `bash /opt/Avaya/ExperiencePortal/Support/SecurityTools/AAEP_FIPS_remove.sh`
 3. 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.
2. On AVL or RHEL8 in FIPS mode, WebLM cannot contact external or local WebLM server using secure connection.
Workaround options:
 - Install the Experience Portal license on the WebLM server that co-resides with the Primary EPM and access that server using http URL connection.
 - or
 - Update the WebLM certificates by following the instructions documented in `WebLMCertificateConfiguration.pdf` under `/opt/Avaya/ExperiencePortal/Support/WebLM` folder

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

Introduced in AEP 8.0 is the ability to upgrade using Avaya Enterprise Linux or RHEL 7.8+ / 8.2+. The key points relating to upgrading to AEP 8.0 are as follows:

- Any versions of Experience Portal prior to 7.2.3 **must first upgrade to latest 7.2.3 before upgrading to 8.0.**
- Supported upgrade paths:
 - AVL based EP deployments
 - EP 6.x -> EP 7.2.3 -> EP 8.0
 - RHEL based EP deployments
 - EP 6.x -> EP 7.2.3 -> EP 8.0
 - OVA based deployments
 - EP 7.2.3 -> EP 8.0
 - In-place OVA upgrades are not supported to 8.0 (for POM support)
 - EP 8.0 OVA(s) must be deployed
- **All** upgrades are based on manual backup and restore of data
- Upgrading directly from EP 6.x to EP 8.0 is not supported
- If custom certificates are configured in the 7.2.3 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 8.0*** (<https://downloads.avaya.com/css/P8/documents/101070956>) 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 7.2.3 up to and including 7.2.3.0.0527 are included in Experience Portal 8.0

This Patch aligns with the POM GA Release. This version is required if POM is to be installed.

ID	Issue	Release found in	Release fixed in
EXPPORTAL-4941	Intermittent issue where vpms service show "failed" when "systemctl status vpms" is run	8.0.0.0.1217	8.0.0.0.1400
EXPPORTAL-5393	cannot add speech server configured in no-default zone in application	8.0.0.0.1217	8.0.0.0.1404
EXPPORTAL-5632	Save on the Change MPP page, incorrectly displays the 'trust certificate' checkbox. With custom identity certificates, ticking this causes the Primary EPM to lose comms with MPP's and EPM's	8.0.0.0.1217	8.0.0.0.1411
EXPPORTAL-5372	Update Tomcat to 8.5.60 for EP, AppServer and MMSServer	8.0.0.0.1217	8.0.0.0.1411
EXPPORTAL-5642	POM lab Customer call gets disconnected with 488 Not Acceptable Here.	8.0.0.0.1217	8.0.0.0.1411
EXPPORTAL-5782	Update postGreSQL to 11.10	8.0.0.0.1217	8.0.0.0.1415
EXPPORTAL-5799	vpms service sometimes takes over 5 minutes to come up, in which case systemctl reports it as "failed" even though it is running	8.0.0.0.1217	8.0.0.0.1415
EXPPORTAL-5645	DTMF received is converted from digit to another value	8.0.0.0.1217	8.0.0.0.1421
EXPPORTAL-5846	EPM/MPP patch setup.sh script fails to stop and start service, SetupServerCertificate and SetDbPassword do not restart mpp	8.0.0.0.1217	8.0.0.0.1421
EXPPORTAL-5371	Unable to invoke VPManagementService from a browser (includes support for j_security_check redirect to https)	8.0.0.0.1217	8.0.0.0.1423
EXPPORTAL-5893	httpd does not start after applying patch 8.0.0.0.1421	8.0.0.0.1421	8.0.0.0.1423
EXPPORTAL-5882	Conference: Max Conference Members Exceeded	8.0.0.0.1217	8.0.0.0.1425
EXPPORTAL-2126	AAEP 7.2 Security Evaluation - Old version of Struts	8.0.0.0.1217	8.0.0.0.1425
EXPPORTAL-5917	ASR behavior broke after upgrading to 7.2.3 from 7.2.1. Propagation to 8.0.0.	8.0.0.0.1217	8.0.0.0.1426
EXPPORTAL-5902	Co-resident AppServer doesn't reinstall after it was uninstalled	8.0.0.0.1217	8.0.0.0.1427
EXPPORTAL-5540	VXML Core Dump	8.0.0.0.1217	8.0.0.0.1428
EXPPORTAL-5926	VB logs write incorrectly when retention increased prop. to 8.0	8.0.0.0.1217	8.0.0.0.1429
EXPPORTAL-6134	Auxiliary OVA deployment fails to start if Primary EPM not running during Aux deployment	8.0.0.0.1217	8.0.0.0.1431
EXPPORTAL-6005	Platform type trusted certificate after upload is not automatically loaded as a trusted certificate at runtime	8.0.0.0.1217	8.0.0.0.1431
EXPPORTAL-6206	Cleartext Transmission of Sensitive Information Login and password being allowed to be sent via http - clear text (prop to 8.0)	8.0.0.0.1217	8.0.0.0.1432
EXPPORTAL-6221	Update apache configuration (vpms.conf) for httpd 2.4 for localhost misconfiguration	8.0.0.0.1217	8.0.0.0.1436
EXPPORTAL-6221	Update apache configuration (mpp.conf) for httpd 2.4 for localhost misconfiguration	8.0.0.0.1217	8.0.0.0.1436

ID	Issue	Release found in	Release fixed in
EXPPORTAL-6022	do_UpdateHost script needs to be updated for systemd backward prop to 8.0	8.0.0.0.1217	8.0.0.0.1436
EXPPORTAL-6141	Dialogflow support for regionalization	8.0.0.0.1217	8.0.0.0.1438
EXPPORTAL-6342	Session manager Core dumped. Propagation to 8.0.0.	8.0.0.0.1217	8.0.0.0.1439
EXPPORTAL-6346	XSS security issues on Avaya Aura Experience Portal 7.2.0	8.0.0.0.1217	8.0.0.0.1440
EXPPORTAL-6356	Saving an EPM or MPP removes Platform cert with chain from conf/truststore	8.0.0.0.1217	8.0.0.0.1441
EXPPORTAL-6357	Dialogflow: Race condition in DTMF guard timer	8.0.0.0.1217	8.0.0.0.1442
EXPPORTAL-6359	Audio isn't passed into conference from one-way join	8.0.0.0.1217	8.0.0.0.1442
EXPPORTAL-6379	Dialogflow: SessionManager core dump when CX response contains mixedAudio with TTS segments	8.0.0.0.1217	8.0.0.0.1442
EXPPORTAL-6380	DTMF issues with EP Test application	8.0.0.0.1217	8.0.0.0.1442
EXPPORTAL-6392	Sip call id unknown in POM OD application prop	8.0.0.0.1217	8.0.0.0.1443
EXPPORTAL-6406	SR:1-17095063638 PEA:1-7VCBZN7 Male TTS voice not played - prop. 8.0.0	8.0.0.0.1217	8.0.0.0.1443
EXPPORTAL-6438	Update Tomcat from 8.5.60 to 8.5.63 prop to 8.0	8.0.0.0.1217	8.0.0.0.1445
EXPPORTAL-6446	activemq sometimes shows stopped state even when running.	8.0.0.0.1217	8.0.0.0.1446
EXPPORTAL-6516	activemq sometimes does not start	8.0.0.0.1217	8.0.0.0.1446
EXPPORTAL-6489	DTMF not recognized. Propagation to 8.0.0.	8.0.0.0.1217	8.0.0.0.1446
EXPPORTAL-6395	SIP incorrect Content-Length value causes core dump	8.0.0.0.1217	8.0.0.0.1446
EXPPORTAL-6433	CCXML browser cache isn't cleared by the "Clear MPP cache" button	8.0.0.0.1217	8.0.0.0.1447
EXPPORTAL-6552	Update Tomcat to 8.5.64	8.0.0.0.1217	8.0.0.0.1448
EXPPORTAL-6582	Async CCAI functionality rendered intermittent by 7.2.3.0.1112. Propagation to 8.0.0.	8.0.0.0.1217	8.0.0.0.1450
EXPPORTAL-6572	Allow the control of the "WaitForSafeExit" timer on the MPPprop to 8.0	8.0.0.0.1217	8.0.0.0.1450
EXPPORTAL-6584	IPC messages delayed on initial connection, Port to 8.0	8.0.0.0.1217	8.0.0.0.1451

Known issues and workarounds

Installation Issues

ID	Minimum conditions	Visible symptoms	Workaround
N/A	Installing or Upgrading Experience Portal Primary or Auxiliary EPM	TLS communications fail with errors like “invalid protocol version” or “protocol_error”	<p>Ensure that the surrounding environment including external servers uses TLS 1.2 protocols for establishing secure communications with Experience Portal.</p> <p>Suggestions</p> <p>External Servers (excluding Enterprise WebLM Servers)</p> <p>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.</p> <ul style="list-style-type: none"> • Java based servers (Application servers including servers hosting Redirector application) <ul style="list-style-type: none"> • 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. <p>Enterprise WebLM Server</p> <p>Enterprise WebLM server which is using an older version of JDK will not be able to allocate licenses to the Local WebLM Server on the Primary EPM using TLS 1.2. In order 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.</p> <p>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:</p> <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> a. Remove -TLSv1 -TLSv1.1 from the SSLProtocol line shown in the section shown below: b. Replace the SSLCipherSuite line with <pre>SSLCipherSuite HIGH:MEDIUM:!ADH:!EDH:!RC4:!MD5:!3DES:!IDEA</pre>

ID	Minimum conditions	Visible symptoms	Workaround
			<pre data-bbox="928 275 1448 552"><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/webmlserver.crt SSLCertificateKeyFile /etc/pki/tls/private/webmlserver.key ProxyPass /WebLM ajp://localhost:3009/WebLM </VirtualHost></pre> <p data-bbox="979 611 1425 663">3. Restart the Apache service using the command “/sbin/service httpd restart”.</p> <p data-bbox="928 709 1455 762">Note: If the system is reinstalled or upgraded to a newer version, these steps need to be re-applied.</p> <p data-bbox="928 791 1474 1062">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.</p>
N/A	Installing or Upgrading Experience Portal Primary EPM in a network environment with DNS and co-residing WebLM server is used for hosting either Enterprise or Allocation licenses.	Local WebLM server does not show any Server Host ID under Server Properties web page. As WebLM server does not have a Server Host ID, installation of a license file fails.	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.
N/A	Enterprise WebLM 7.1 OVA	Experience Portal is unable to acquire licenses from WebLM 7.1 OVA. avaya.vpms.log has the exception “Problem with connection to server: sun.security.validator.ValidatorException: No trusted certificate found”	To work around this issue, import the new public security certificate of Enterprise WebLM 7.1 OVA in the truststore used by the WebLM client. <ol data-bbox="979 1654 1481 1934" style="list-style-type: none"> 1. Log into the Primary EPM as a user with root privileges. 2. Copy the Enterprise WebLM 7.1 public certificate to the Primary EPM. (Say weblm71ova.pem) 3. Run the command \$JAVA_HOME/bin/keytool -keystore \$CATALINA_HOME/webapps/VoicePortal/WEB-INF/lib/trusted_weblm_certs.jks -

ID	Minimum conditions	Visible symptoms	Workaround
			importcert -v -alias weblm71ova -file <file location>/weblm71ova.pem
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.
N/A	Cannot install from path that contains space	If attempting to mount the Experience Portal image and perform an install from that location the install will fail if the location contains a directory path that contains a space character.	Before starting the install, make sure that none of the directory names in the path to the install Experience Portal contain a space.
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. "
NA	FIPS is enabled	AEP 8.0 - License server does not connect	<ul style="list-style-type: none"> • Install the Experience Portal license on the WebLM server that co-resides with the Primary EPM and access that server using the http URL connection or • Update the WebLM certificates by following the instructions documented in

ID	Minimum conditions	Visible symptoms	Workaround
			WebLMCertificateConfiguration.pdf under Support/WebLM folder
EXPPORTAL-3645	IPv6 environment	AEP 8.0 - IPv6 license server does not connect	<ul style="list-style-type: none"> 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 Install the Experience Portal license on an external WebLM server that is accessible via IPv4
EXPPORTAL-3623		How “DTMF Type Ahead Enabled” filed affect to application.	
EXPPORTAL-3569		Appearing files avaya.upgrade.*.psql.err and file avaya.upgrade.*.psql.err.filt after upgrade EPM	
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
EXPPORTAL-4555		Running command “ systemctl mpp status ” after mpp service has been stopped, shows “Failure”	If you stop mpp running command: systemctl mpp stop and then run command: “ systemctl mpp status ” the status shows as “ Failed ” rather than “ Stopped ”. This has no impact on the stopping or starting of mpp no error messages are displayed when stopping or starting the mpp.
EXPPORTAL-4807		Incoming Web services from EP to MPP use TLS rather than MTLS	EP->MPP link is still secure, the difference is that the EP client cert is not validated on MPP. However, the MPP cert is validated on EP.
SMGR-54468		Cannot use FIPS SMGR as a CA	<ol style="list-style-type: none"> Add EPM as an End Entity on SMGR Security with Token Type = JKS. Create Keystore and download the JKS certificate. Cope the JKS certificate to the EPM server and run the Keytool command to convert the JKS certificate to a p12 certificate. Convert the JKS to p.12: <pre>keytool -importkeystore -srckeystore <end_entity_name>.jks -destkeystore pkcs_filename.p12 -srcalias <end_entity_name> -srcstoretype JKS -deststoretype PKCS12 -</pre>

ID	Minimum conditions	Visible symptoms	Workaround
			<p>deststorepass <PKCS12_password> -srcstorepass <end_entity_password></p> <p>5. Use the SetupServerCertificate.sh -import command and follow steps to install custom p12 certificate.</p>
EXPPORTAL-4545	Limit the number of Root generations without restarting the EP servers	If using default certificates (EPM Root signing enabled), multiple invocations of Root generate without restarting the EP servers (EPM's or MPP's) will cause communication between the servers to be lost.	<p>Ensure that the EP servers in the solution are restart immediately after generating a new EPM Root certificate.</p> <p>If communication has been lost;</p> <ol style="list-style-type: none"> 1) Run setup_vpms.php on the Auxiliaries and MPP's <p>If Primary EPM cannot be controlled through web interface EPM Manager, restart the Primary EPM through command line</p>
EXPPORTAL-4623	Auxiliary EPM Identity Certificate is not updated when displayed in Security -> Certificates -> EPM Identity Certificates	<p>If the Auxiliary EPM Identity Certificate has changed either through;</p> <ol style="list-style-type: none"> 1) Generating a new Root, restarting the Auxiliary, which in turn generates a new Root signed identity 2) Import a custom identity certificate using the SetupServerCertificate.sh script <p>The Security -> Certificates -> EPM Identity Certificate page displays the old identity certificate.</p>	<p>To get the page to display the new Identity Certificate go to EPM Servers and click on the link for the Auxiliary server.</p> <p>This is a display issue, operationally for secure communications the Auxiliary is using the new Identity Certificate.</p>
EXPPORTAL-4518	Intermittent issue post Root generation if Primary / Aux / MPP are restarted at the same time	After Root generation, if the Primary EPM is restarted at the same time as an Auxiliary EPM or an MPP, the Auxiliary and the MPP may not generate a new Root signed identity certificate	<p>To prevent this, after Root generation, ensure that the Auxiliary EPM's and the MPP's are always restarted before the Primary EPM. Only restart the Primary EPM after the Auxiliary EPM's and the MPP's go back into the running state post restart.</p> <p>If the issue does happen, communication with the Auxiliary and MPP will continue to use an identity certificate signed by the old Root. This can cause communication issues down the line – to resolve, run setup_vpms.php on the Aux or MPP.</p>
EXPPORTAL-3566	Bridge transfer fails	When a bridge transfer option is selected it asks for a number to transfer to. Following the entry of the valid number the destination phone rings but on answer the call drops with message "failed for unknown reason".	N/A

Avaya Linux 8.2 Issues

ID	Minimum conditions	Visible symptoms	Workaround
EXPPORTAL-4936 Fixed in RH8.2.64-AV14EP8	Leave the DNS Domain field empty on new install when using drop 12 of AVL	See the hostname after install of # hostname -f ???????.none	As Root execute: # sed -i "s/\.none\s//g" /etc/hostname # hostnamectl set-hostname \$(cat /etc/hostname)
N/A	Using the "Red Hat Enterprise Linux 8 (64-bit)" template in VMware 6,7	Cannot boot from ISO, will display "EFI ???... Unsuccessful	In the VM Options -> Boot Options change the Firmware from EFI to BIOS

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 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.	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 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	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.

ID	Minimum conditions	Visible symptoms	Workaround
	different IP addresses		
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 on 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-2723	Use SMGR 8.x for SSO	Experience Portal is missing in SMGR 8.x web console	Use SMGR 7.x if Single Sign On is required
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.
EXPPORTAL-4876	Replacing default EP Signing certificate with 3 rd Party signed certificate	Security -> Certificates -> EP Signing Certificate tab ->Certificate Signing Request tab -> Upload . Using this method to replace the default EP Signing Certificate does not place the CA trusted root Certificate to the Tomcat truststore and Apache trusted directory which will cause any connection to not trust the EP Signing Certificate	Replacing the EP Signing certificate is not a commonly required step in configuring a working AEP, but if the customer insists on doing so then use the alternative means to upload the 3 rd Party signed EP Signing certificate via the Security -> Certificates -> EP Signing Certificate tab ->Certificate tab -> Upload . This will place all the necessary elements on the EPM server.
EXPPORTAL-4609	Co Res issue only New feature in Certificate Simplification deliverable – No manual confirmation of trusting a new certificate.	When adding Aux or Co-Res MPP the certificate that is downloaded is the EPM Root signed identity certificate - this should be auto trusted and not require the user to check the trust checkbox. When first adding a standalone MPP, the identity certificate that is downloaded is the self-signed MPP identity certificate. This would need to be manually trusted by the user.	User must manually trust the certificate.
EXPPORTAL-4945	Using Google Dialogflow	early_media reject code removed accidentally in Dialogflow root.js	In the case of early media, if the VXML implementer wants to reject the call, the call does not get rejected with a 480 "Early media hangup". But the call is still disconnected.
N/A	Axis2 listServices	Due to security concerns EPM no longer lists the Axis2 web Services the product supports.	None.

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.