Avaya Aura® Experience Portal 7.2.3 - Release Notes

7 February 2020

Contents

Document changes

Date	Description
February 7th, 2020	GA Patch version for AAEP 7.2.3

Introduction

This document provides late-breaking information to supplement Avaya Aura® 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 Aura® Experience Portal management web pages may also be available on the Avaya Support site at http://support.avaya.com.

Installation

Product compatibility

Note the following limitations.

Application	Compatibility Description	Recommendation
Proactive Outreach Manager (POM)	POM is a managed application (administration runs on the EPM). Interoperability issues with older POM releases due to currency changes introduced in AAEP 7.2. POM 3.1 supports the updated currency requirements.	If using POM, You must use POM 3.1 or later release that supports Experience Portal 7.2.3.
Intelligent Call Routing (ICR)	ICR is a managed application (administration runs on the EPM). Inter Interoperability issues with older ICR releases due to currency changes introduced in AAEP 7.2. ICR 7.0.2 supports the updated currency requirements.	If using ICR, You must use ICR release that supports Experience Portal 7.2.3. Note: Refer to PSN005504u if you are making a fresh install of ICR
Call Back Assist (CBA)	CBA is a packaged application (communicates with EP via web services). Compatibility issues due to Security (TLS 1.2 support) changes introduced in AAEP 7.2. CBA 4.6.1 supports TLS 1.2 and AAEP 7.2.	If using CBA, You must use CBA release that supports Experience Portal 7.2.3.

Dynamic Self Service (DSS)	DSS is a packaged application (communicates with EP via web services). Compatibility issues due to Security (TLS 1.2 support) changes introduced in AAEP 7.2. DSS 2.9.2 supports TLS 1.2 and EP 7.2.	If using DSS, You must use DSS release that supports Experience Portal 7.2.3.

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

Required patches

Find interoperability and compatibility information at the following location: https://support.avaya.com.

Experience Portal 7.2.3 is delivered as a patch on an existing Experience Portal 7.2.0, 7.2.1 or 7.2.2 system.

When installing or upgrading to Experience Portal 7.2.3, it is required to install the latest patches available. Check https://support.avaya.com for the latest MPP and EPM patches. See the table below for specific patch requirements.

Download ID	Patch	Notes
AAEP0000143 **AAEP0000144**	7.2.3.0.0505.tar.gz 7.2.3.0.0505.tar.gz.sig OR a newer patch.	Patch for the MPP portion of the product.
AAEP0000145	EPM-7.2.3.0.0505.tar.gz OR a newer patch.	Patch for the EPM portion of this product, it also includes patches, currency and documentation updates, this patch should also be applied to MPP system to update the mms server if required.
AAEP0000133	epavl-7.2.0.0.1910.tar.gz	AVL 7.2.x Quarterly Security Patch, check on support.avaya.com for newer versions of this patch.
AAEP0000121	AVL_FIPS_dracut.tgz	Package required to put RHEL 6.8 into FIPS mode. For users of OVA or Avaya supplied hardware. Software only customers need to contract Red Hat for equivalent downloads - See How can I make RHEL 6 or RHEL 7 FIPS 140-2 compliant?

File list - Avaya Aura® Experience Portal 7.2 software

Filename	Modification time stamp	File size	Version number
AAEP-7.2.0.0.1117.iso	**6/21/2017 19:58**	**3,007,021,056**	**7.2.0.0.1117**

Filename	Modification time stamp	File size	Version number
AAEP-7.2.0.0.1117.iso.sha256.sig	6/21/2017 19:59	256	7.2.0.0.1117
Avaya_Public_Certificate.crt			

All Avaya Aura® Experience Portal 7.2 software packages are protected via code signing. The SHA256 hash is generated and signed by the Avaya File Signing Authority for each Avaya Aura® Experience Portal 7.2 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
AAEP-7.2.0.0.1117.iso	This is the Avaya Aura® Experience Portal 7.1 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 Aura® Experience Portal 7.2 ISO Image: **sha256sum AAEP-7.2.0.0.1117.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 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.crt > pubkey.pem** • Create the SHA256 of the ISO **sha256sum AAEP-7.2.0.0.1117.iso > AAEP-7.2.0.0.1117.iso.sha256** • Verify the SHA256 hash signature using the public key “pubkey.pem” and SHA256: **openssl dgst -sha256 -verify pubkey.pem -signature AAEP-7.2.0.0.1117.iso.sha256.sig AAEP-7.2.0.0.1117.iso.sha256** “Verified OK” from the above command indicates the SHA256 hash signature is valid.

File list - Avaya Aura® Experience Portal 7.2 OVA software

Filename	Modification time stamp	File size	Version number
ExperiencePortal-AuxiliaryEPM-7.2.0.0.1117-e55-1.ova	6/21/2017 22:17	6,690,600,960	7.2.0.0.1117
ExperiencePortal-AuxiliaryEPM-7.2.0.0.1117-e55-1.sha256sum.sig	6/21/2017 22:01	256	7.2.0.0.1117
ExperiencePortal-MPP-7.2.0.0.1117-e55-1.ova	6/21/2017 22:04	4,583,976,960	7.2.0.0.1117
ExperiencePortal-MPP-7.2.0.0.1117-e55-1.sha256sum.sig	6/21/2017 21:53	256	7.2.0.0.1117

Filename	Modification time stamp	File size	Version number
ExperiencePortal-PrimaryEPM-7.2.0.0.1117-e55-1.ova	6/21/2017 22:20	7,746,713,600	7.2.0.0.1117
ExperiencePortal-PrimaryEPM-7.2.0.0.1117-e55-1.sha256sum.sig	6/21/2017 22:02	256	7.2.0.0.1117
Avaya_Public_Certificate.crt			

All Avaya Aura® Experience Portal 7.2 OVA software packages are protected via code signing. The SHA256 hash is generated and signed by the Avaya File Signing Authority for each Avaya Aura® Experience Portal 7.2 OVA 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
ExperiencePortal-PrimaryEPM-7.2.0.0.1117-e55-1.ova	This is the Avaya Aura® Experience Portal 7.2 Primary EPM OVA 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 Aura® Experience Portal 7.2 Primary EPM OVA ISO Image: **sha256sum ExperiencePortal-PrimaryEPM-7.2.0.0.1117-e55-1.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 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.crt > pubkey.pem** • Create the SHA256 of the ISO **sha256sum ExperiencePortal-PrimaryEPM-7.2.0.0.1117-e55-1.iso > ExperiencePortal-PrimaryEPM-7.2.0.0.1117-e55-1.sha256sum** • Verify the SHA256 hash signature using the public key "pubkey.pem" and SHA256: **openssl dgst -sha256 -verify pubkey.pem -signature ExperiencePortal-PrimaryEPM-7.2.0.0.1117-e55-1.sha256sum.sig ExperiencePortal-PrimaryEPM-7.2.0.0.1117-e55-1.sha256sum** "Verified OK" from the above command indicates the SHA256 hash signature is valid.
ExperiencePortal-AuxiliaryEPM-7.2.0.0.1117-e55-1.ova	This is the Avaya Aura® Experience Portal 7.2 Auxiliary EPM OVA 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 Aura® Experience Portal 7.2 Auxiliary EPM OVA ISO Image: **sha256sum ExperiencePortal- AuxiliaryEPM -7.2.0.0.1117-e55-1.iso** 4. 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 image is not corrupted. 5. 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.crt > pubkey.pem** • Create the SHA256 of the ISO **sha256sum ExperiencePortal-AuxiliaryEPM-7.2.0.0.1117-e55-1.iso > ExperiencePortal-AuxiliaryEPM-7.2.0.0.1117-e55-1.sha256sum** • Verify the SHA256 hash signature using the public key “pubkey.pem” and SHA256: **openssl dgst -sha256 -verify pubkey.pem -signature ExperiencePortal-AuxiliaryEPM-7.2.0.0.1117-e55-1.sha256sum.sig ExperiencePortal-AuxiliaryEPM-7.2.0.0.1117-e55-1.sha256sum** “Verified OK” from the above command indicates the SHA256 hash signature is valid.
ExperiencePortal-MPP-7.2.0.0.1117-e55-1.ova	This is the Avaya Aura® Experience Portal 7.2 MPP OVA 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 Aura® Experience Portal 7.1 MPP OVA ISO Image: **sha256sum ExperiencePortal- MPP -7.2.0.0.1117-e55-1.iso** 6. 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 image is not corrupted. 7. 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.crt > pubkey.pem** • Create the SHA256 of the ISO **sha256sum ExperiencePortal-MPP-7.2.0.0.1117-e55-1.iso > ExperiencePortal-MPP-7.2.0.0.1117-e55-1.sha256sum**

	• Verify the SHA256 hash signature using the public key “pubkey.pem” and SHA256: **openssl dgst -sha256 -verify pubkey.pem -signature ExperiencePortal-MPP-7.2.0.0.1117-e55-1.sha256sum.sig ExperiencePortal-MPP-7.2.0.0.1117-e55-1.sha256sum** “Verified OK” from the above command indicates the SHA256 hash signature is valid.

File list - Avaya Enterprise Linux for Avaya Aura® Experience Portal 7.2 software

Filename	Modification time stamp	File size	Version number
AvayaLinux-RH6.8.64-AV07EP72.30May17.194049.iso	May 30 16:40	1,138,196,480	RH6.8.64-AV07EP72
AvayaLinux-RH6.8.64-AV07EP72.30May17.194049.sha256.sig	May 31 15:08	256	RH6.8.64-AV07EP72
Avaya_Public_Certificate.crt			

All Avaya Enterprise Linux for Avaya Aura® Experience Portal 7.2 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 Aura® Experience Portal 7.2 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-RH6.8.64-AV07EP72.30May17.194049.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: **sha256sum AvayaLinux-RH6.8.64-AV07EP72.30May17.194049.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 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.crt > pubkey.pem** • Create the SHA256 of the ISO **sha256sum AvayaLinux-RH6.8.64-AV07EP72.30May17.194049.iso > AvayaLinux-RH6.8.64-AV07EP72.30May17.194049.iso.sha256**

	• Verify the SHA256 hash signature using the public key "pubkey.pem" and SHA256: **openssl dgst -sha256 -verify pubkey.pem -signature AvayaLinux-RH6.8.64-AV07EP72.30May17.194049.iso.sha256.sig AvayaLinux-RH6.8.64-AV07EP72.30May17.194049.iso.sha256** "Verified OK" from the above command indicates the SHA256 hash signature is valid.

Backing up the software

Important: Before starting an upgrade, you should back up your existing Avaya Aura® 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.

Important: For upgrades from Experience Portal 7.1 to Experience Portal 7.2, the operating system upgrade is mandatory. The following Linux versions are supported for Experience Portal 7.2:

- Red Hat Enterprise Linux Release 6.6 64 bit or later but not RHEL 7.x
- Avaya Enterprise Linux RH6.8.64-AV07EP72 or later

Note: Avaya recommends that you upgrade to RHEL 6.8 or the Avaya Linux based on RHEL 6.8 to avail the security fixes.

For detailed upgrade and backup procedures, see the Avaya Technical Support Web site https://support.avaya.com and the document titled "***Upgrading to Avaya Aura® Experience* Portal 7.2***"*. (https://downloads.avaya.com/css/P8/documents/101039773)

Installing the release

Important: Before installing or upgrading Avaya Aura® 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 Aura® Experience Portal on multiple servers***" *(https://downloads.avaya.com/css/P8/documents/101039769) or "**Implementing Avaya Aura® Experience Portal on a single server**" (https://downloads.avaya.com/css/P8/documents/101039771)*. Or for upgrades see the document *"**Upgrading to Avaya Aura® Experience Portal 7.2**". (https://downloads.avaya.com/css/P8/documents/101039773)*

For detailed OVA installation and upgrade procedures, see the Avaya Technical Support Web site https://support.avaya.com and the document titled "***Deploying Avaya Aura® Experience Portal in an Avaya Customer Experience Virtualized Environment***" *(https://downloads.avaya.com/css/P8/documents/101039763)*.

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 Aura® Experience Portal***" (*https://downloads.avaya.com/css/P8/documents/101039767*).

Restoring software to previous version

For detailed procedures on restoring software to a previous version, see the Avaya Technical Support Web site https://support.avaya.com and the document titled "***Upgrading to Avaya Aura® Experience Portal 7.2***". (*https://downloads.avaya.com/css/P8/documents/101039773*).

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 Aura® Experience Portal 7.2 and is cumulative since the last major/minor release showing the most recent release first and oldest release last.

* New in AAEP 7.2.3

Enhancement	Description
Google Dialogflow/CC AI (Note capacity limitations above)	• * 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	• * 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
POM	• * Scheduled reports for POM can be executed in 15 and 30 minute intervals
General	• * Request-URIs can be prioritized over "to" headers
SMS	• Support for two-way MMS with Avaya Zang connections. • Support i2SMS for outbound SMS. • Allow Avaya Ava to receive and reply to SMS via Experience Portal • Integration of Avaya Zang as a new HTTP connector for two-way SMS. • Support SMPP connections over TLS 1.2.
Reporting	• 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	• * Nuance Recognizer 11 (ASR) for Conversational Speech using Dragon Voice add-on • * Vocalizer 7 (TTS)

Enhancement	Description
	• * 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	• 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.
Global CAVs	• Ability for administrators to configure the user defined global Configurable Application Variables. These are system wide variables that are not specific to any particular application.
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 Aura® Experience Portal system to address security vulnerabilities in prior TLS versions. • Scripts SetupServerCertificate.sh and ImportExternalServerCertificate.sh provide the

Enhancement	Description
	functionality previously provided by GenerateServerCertificate.sh & ImportServerCertificate.sh. • $AVAYA_HOME/Support/Security-Tools – New folder for certificate scripts and EASG related scripts.
Currency Updates	• * VMWare ESXi 6.7 • * Tomcat 8.5.42 • * PostgreSQL 11.4 • * Jasper Reports 6.6.0
Interoperation	• Aura 8.0, 8.0.1 support, See EXPPORTAL-2723 For limitations.
Platform	• * Avaya Common Server (ACP) 110 and 130 support
EASG	• Enhanced Access Security Gateway (EASG) EASG provides a secure method for Avaya services personnel to access the Avaya Aura® 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 Healthcheck. • 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

Enhancement	Description
	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 Aura® Experience Portal Overview and Specification***" *(https://downloads.avaya.com/css/P8/documents/101060145)*.

Fixes

The following table is cumulative since the last major/minor release showing the most recent release first and oldest release last.

ID	Minimum Conditions	Visible symptoms	Release found in	Release fixed in
EXPPORTAL-450	Folder of EP backups contains a folder or file with the substring "pkg".	Restore fails.	7.0.2.0	7.2.1.0
EXPPORTAL-1399	Zang SMS processor is switched from primaryEPM to AuxEPM or vice versa.	The last incoming message is processed by EP twice.	7.2.0.0	7.2.1.0
EXPPORTAL-1501	Run MySQL upgrade script.	VPAppLog upgrade script reports an error, if the database was configured for case-sensitive table names. New Application generated logs will not be added to the VPAppLog table.	7.2.0.0	7.2.1.0
EXPPORTAL-1503	Name is configured in multi-byte language.	Application name is incorrect in reports for voice calls.	7.2.0.0	7.2.0.0 post GA patch & 7.2.1.0
EXPPORTAL-1508	Heavy use of async fetch (POM applications).	CCXML core dump.	7.2.0.0	7.2.0.0 post GA patch & 7.2.1.0
EXPPORTAL-1509	First SMS response for a newly created Zang connection.	2 CDR records are created.	7.2.0.0	7.2.1.0
EXPPORTAL-1516	Stray RTP packets after codec renegotiation when G.711 packet loss concealment is running. This can especially occur when an RTP packet with a non-G.711 type is decoded as though it were G.711 (shuffling is a catalyst for this).	Buffer overflow resulting in MediaManager core dump..	7.2.0.0	7.2.0.0 post GA patch & 7.2.1.0
EXPPORTAL-1517	POM running heavy load.	CCXML core dump.	7.2.0.0	7.2.0.0 post GA patch & 7.2.1.0
EXPPORTAL-1519	Conference joins that fail because the system limit for either the maximum number of talkers or listeners is reached.	MediaManager core dump.	7.2.0.0	7.2.0.0 post GA patch & 7.2.1.0

ID	Minimum Conditions	Visible symptoms	Release found in	Release fixed in
EXPPORTAL-1524	HTTP fetch is redirected.	Voice Browser deadlocks on next attempt to fetch the same resource..	7.2.0.0	7.2.0.0 post GA patch & 7.2.1.0
EXPPORTAL-1533	Sending messages greater than 160 characters using Avaya Zang	Large Messages fail.	7.2.0.0	7.2.0.0 post GA patch, 7.2.1.0 & 7.2.3.0
EXPPORTAL-1535	CCXML conference with both G.729 and G.729B participants.	Media Manager core dump.	7.2.0.0	7.2.0.0 post GA patch & 7.2.1.0
EXPPORTAL-1536	EPM logging sync errors for Aux server	Errors in log.	7.2.0.0	7.2.3.0
EXPPORTAL-1537	Heavy use of async fetch (POM applications).	CCXML core dump.	7.2.0.0	7.2.0.0 post GA patch & 7.2.1.0
EXPPORTAL-1542	Specific scenarios when no cache and no-store are used for redirect URI.	VB Redirect to https fails.	7.2.0.0	7.2.0.0 post GA patch & 7.2.1.0
EXPPORTAL-1549	VoiceXML browser needs to support SNI header when configured for TLS	Customer GRIP	7.2.1.0	7.2.1.0 & 7.2.3.0
EXPPORTAL-1552	Managed upgrade against a MPP without running the DownloadPK.bash script.	Upgrade hangs waiting on MPP download. Should error out.	7.2.0.0	7.2.1.0
EXPPORTAL-1557	System has patch installed.	Cannot restore.	7.2.0.0	7.2.1.0
EXPPORTAL-1587	Zang SMS Inbound connection	Greater than 15 seconds to retrieve Zang SMS messages.	7.2.0.0	7.2.1.0
EXPPORTAL-1588	fetchaudiodelay property is set to zero and the fetch audio playing is of a short duration.	Media Manager core dump.	7.2.0.0	7.2.0.0 post GA patch & 7.2.1.0
EXPPORTAL-1606	Custom Application Summary Report	"Sessions from Custom Report" filter in an Application Summary custom report was not saved in subsequent runs.	7.1.0.1	7.2.1.0

ID	Minimum Conditions	Visible symptoms	Release found in	Release fixed in
EXPPORTAL-1609	HTTPS fetch where the Transfer-Encoding header is omitted in the response and the TLS connection is closed with an unclean shutdown.	bad.fetch error in Voice Browser even when the fetch actually did succeed.	7.2.0.0	7.2.1.0
EXPPORTAL-1610	POM sending email.	intermittent "app not configured" error when sending email or SMS.	7.0.1.0	7.2.1.0
EXPPORTAL-1611	OPTIONS poll to a speech server times out but the connection is immediately re-established.	Erroneous PMRCP00008 log events.	7.1.0.1	7.2.1.0
EXPPORTAL-1657	Voice browser refreshes an expired cached prompt file.	Media Manager core dump.	7.2.0.0	7.2.0.0 post GA patch & 7.2.1.0
EXPPORTAL-1660	Incorrect end date in scheduled report with Last Week option.	The End Date header in a scheduled report can be incorrect when a report timeframe of “Last Week” is chosen. This only occurs if the report is generated on a date where the proper report end date is not in the current month. The content of the report is correct, but the End Date header is incorrect.	6.0.0.0	7.2.1.0
EXPPORTAL-1664	Timing conditions with an H.323 station where the media codec has changed between successive calls. Timing conditions with a VXML dialog being terminated while a prompt is playing.	Media Manager core dump.	7.2.0.0	7.2.0.0 post GA patch & 7.2.1.0
EXPPORTAL-1669	Zang SMS message contains “&” character.	Outbound SMS message is truncated.	7.2.0.0	7.2.1.0
EXPPORTAL-1671	View system monitor.	System Monitor status always has a “Running” state for inbound HTTP SMS connections. The status should change to “Error” or “Degraded” if a serious polling error occurs	7.2.0.0	7.2.1.0
EXPPORTAL-1695	CCXML consultative transfer or merge fails and the subsequent re-INVITE (sent to reassert the SDP state prior to the REFER) receives a 491 response.	MPP drops call.	7.1.0.1	7.2.1.0

ID	Minimum Conditions	Visible symptoms	Release found in	Release fixed in
EXPPORTAL-1697	Role name field containing space.	Cannot edit a role.	7.2.0.0	7.2.1.0
EXPPORTAL-1698	On EPM setting page, user provides a password containing exclamation mark.	Entry fails.	7.2.0.0	7.2.1.0
EXPPORTAL-1701	VXML Dialog using “senddigit” function is attached to a CCXML conference.	SessionManager core dump.	7.0.1.0	7.2.1.0
EXPPORTAL-1705	http://<epm ip>/webservices/CompMgrWS shows a directory listing			
EXPPORTAL-1710	VXI browser cache is cleaned frequently.	Media Manager core dump.	7.2.0.0	7.2.0.0 post GA patch & 7.2.1.0
EXPPORTAL-1748	On receiving a re-invite without SDP, MPP offers the previously negotiated SDP instead of a full SDP offer	An inbound call is received by MPP and accepted over SIP, media is negotiated (INVITE - 200 OK). The call is placed on hold by the remote end (Cisco CCM), a re-invite with SDP a=inactive is received, 200 OK response sent. A re-invite is then received by MPP without SDP to take the call off hold. MPP sends out the previously negotiated SDP (hold SDP) in the SDP offer of the 200 OK. The call remains on hold incorrectly.	7.2.0.0	7.2.3.0
EXPPORTAL-1753	second try DTMF collect returns early	Customer has a script with Maximum 15 digits allow for DTMF When first trial(12 digits) failed to pass the customer validation, the script as for a second try , even "#" not input MPP would still return when only 3 digits being poped.	7.2.0.0	7.2.3.0
EXPPORTAL-1773	Forward port fix for error message when joining external database	Go to Data Storage Settings web page and configure Oracle as the external database. Add an SMS or Email processor and then go back to Data Storage Settings web page. The VPMediaServerMgr throws an error "Invalid conversion requested".	7.1.0.0	7.2.3.0

ID	Minimum Conditions	Visible symptoms	Release found in	Release fixed in
EXPPORTAL-1776	40 sec Delay between SessMgr Get Response from ASR and Send Result To VXI	Delay in calls	7.2.0.0	7.2.3.0
EXPPORTAL-1778	Intermittent recordings contain only static	Intermittent recordings from caller for after call survey contained only static.	7.2.0.0	7.2.3.0
EXPPORTAL-1839	Dynamic allocation of ASR ports : Feature Phase 1	Late acquisition of Nuance licenses during a call. Will only acquire an ASR port if the VXML script requires it.	7.2.1.0	7.2.3.0
EXPPORTAL-1927	Experience Portal shall support ability to clamp (block) DTMF in one direction only	Agent and customer are on call. The requirement is to block any DTMF the customer is entering so the Agent does not hear it, but to allow the Agent to enter DTMF to navigate the customer through menus.	7.2.1.0	7.2.3.0
EXPPORTAL-1930	core dumps generated on all MPP - vxmlmgr	MPP degraded, core dumps generated on all MPP – vxmlmgr	7.2.1.0	7.2.3.0
EXPPORTAL-1950	Validation for duplicate DNIS for a voice application is inconsistent	Scenario: For an application, it is possible to add a range number, i.e. 10001 ~ 10002, then add 10002 again in DNIS field. However, if one adds 10002 first, then add 10001~10002, the web page will give a duplicate number error. Validation for duplicate DNIS needs to be removed for this scenario as well.	7.2.0.0	7.2.3.0
EXPPORTAL-1951	No second URL entry box when configuring SMS application with failover or load balance option	No second URL entry box when configuring SMS application with failover or load balance option.	7.2.1.0	7.2.3.0
EXPPORTAL-1966	Consultation query over ASR license	When PC VP connector is used and ccxml application is invoked	7.0.2.0	7.2.3.0
EXPPORTAL-1974	MPP's process restarted and observed core dumps on three MPP on component: SessionManager.	MPP’s process restarted and observed core dumps on three MPP on component: SessionManager	7.1.0.1	7.2.3.0
EXPPORTAL-1984	1-13872001736 - 1-6DUS8MD - SNMP No Such Name Error	There are 2 faults in the Experience Portal 7.x SNMP: The AV-VOICE-PORT-MIB MIB presents errors and modifies the MIB but the values of the calls are not correct.	7.1.0.1	7.2.3.0
EXPPORTAL-1993	change to the handling of termchar is slowing response of the application	AEP 7.2, change to handling of termchar is slowing response of the application	7.2.0.0	7.2.3.0

ID	Minimum Conditions	Visible symptoms	Release found in	Release fixed in
EXPPORTAL-2056	mpp ccxml memory leak due to logging of large data size	Customer reported issue of mpp ccxml memory leak during normal operation:	7.1.0.0	7.2.3.0
EXPPORTAL-2066	Client certificate authentication feature fails on AUX EPM	Client certificate authentication feature fails on AUX EPM	7.2.0.0	7.2.3.0
EXPPORTAL-2067	Privilege Escalation -A specific user type is able to perform functions meant for higher privileged user types by manipulation of user parameters or cookies	Found via security scan.	7.2.1.0	7.2.3.0
EXPPORTAL-2075	Verify does not work for Backup on Windows (if backup folder has comma or backup user has backslash)	If you add a , to the backup folder or a \ to the username when you click verify the field disappears and the verify fails as the mount can't be completed with that missing data. The backups work but the verify fails. The verify does not fail in 7.1 but does in 7.2 or 7.2.1.	7.2.1.0	7.2.3.0
EXPPORTAL-2115	core dumps generated on all MPP - vxmlmgr	Avaya MPP constantly crashing with QOMS_00096: Media Server unexpectedly entered the degraded state alarms	7.2.1.0	7.2.3.0
EXPPORTAL-2128	MediaManger cores seen	Not able to reach IVR, busy tone experience.	7.2.0.0	7.2.3.0
EXPPORTAL-2140	AAEP patch: provide merge function for files shared with POM	AAEP patch install will remove POM additions to the vpmsMsgCode.properties and vpmsAlarmCode.properties files.	7.2.1.0	7.2.3.0
EXPPORTAL-2306	Transcoding from Wave-PCM to Wave-alaw performed with distortion	Distortion found in audio.	7.2.1.0	7.2.3.0
EXPPORTAL-2350	The # doesn't work after the upgrading AAEP to version 7.2.1.0622. propagation to trunk	The termchar is not returned in the DTMF result.	7.2.1.0	7.2.3.0
EXPPORTAL-1606	Preserve "Sessions from Custom Report" filter in an Application Summary custom report		7.2.1.0	7.2.3.0
EXPPORTAL-1549	VoiceXML browser needs to support SNI header when configured for TLS		7.2.1.0	7.2.3.0
EXPPORTAL-1609	AVB returns bad.fetch when app. server does not give transfer-encoding with chunked		7.2.0.0	7.2.3.0

ID	Minimum Conditions	Visible symptoms	Release found in	Release fixed in
EXPPORTAL-1610	intermittent "app not configured" error when sending email		7.0.1.0	7.2.3.0
EXPPORTAL-2363	Remove G722 Codec from the default lost of Codecs		7.2.2.0	7.2.3.0
EXPPORTAL-2317	SR 1-14430050018 PEA 1-6NIDSZP - Sync error with Aux EPM server		7.2.1.0	7.2.3.0
EXPPORTAL-2416	Prompt Transcoding background noise		7.2.1.0	7.2.3.0
EXPPORTAL-2470	EP VB message out of sequence		7.2.1.0	7.2.3.0
EXPPORTAL-2126	AAEP 7.2 Security Evaluation - Old version of Struts	Security scan will show venerable version of Struts on system	7.2.0.0	7.2.3.0
EXPPORTAL-2477	MPP doesn't update params when resuming the call		7.2.1.0	7.2.3.0
EXPPORTAL-2452	HOSTNAME in system and SNMP queries returns "EPM"		7.2.1.0	7.2.3.0
EXPPORTAL-2201	Unencrypted private key store in the database		7.2.1.0	7.2.3.0
EXPPORTAL-2199	Unused file being tagged as a security issue on a site	Security scan will show venerable version of $CATALINA_HOME/webapps/axis/WEB-INF/users.lst on system	7.2.1.0	7.2.3.0
EXPPORTAL-2712	UCID corrupt		7.2.0.0	7.2.3.0
EXPPORTAL-2747	Prop from 7.1 'ASR' result for DTMF no-match		7.1.0.0	7.2.3.0
EXPPORTAL-2830	Propagation EXPPORTAL-2460 Default error handler no longer heard when app is unreachable; system hangs up right away and reports success		7.2.2.0	7.2.3.0
EXPPORTAL-2846	Automate Postgres 11 password hashing change using new script		7.2.1.0	7.2.3.0
EXPPORTAL-2878	After installing 7.2.1+, cannot restore the backup from 7.0.2	Error Message: You cannot restore a backup taken from a version 7.X.X.0.0XXX on a version 7.2.X.0.XXX system. Restore operation aborted!	7.2.2.0	7.2.3.0

ID	Minimum Conditions	Visible symptoms	Release found in	Release fixed in
		See PSN005433u		
EXPPORTAL-2950	Message status shows -999 when sending SMS greater than 160 characters via Zang	The "Message Status" column in the Contact Detail Report shows -999 when sending SMS greater than 160 characters via Zang even though the message is broken into multiple messages (<160 characters) and delivered successfully to the handset. POM completion codes are also impacted.	7.2.1.0	7.2.3.0
EXPPORTAL-3042	Audio file is playing from cache		7.2.2.0	7.2.2.0 7.2.3.0
EXPPORTAL-3057	Incorrect end date in on-demand report with Last Week option, if run during first week of month	The End Date in an on-demand report can be incorrect when a report timeframe of “Last Week” is chosen	7.2.2.0	7.2.3.0
EXPPORTAL-3059	dtmf result is not what customer expected, propagation to EP7.2.3	input 99991234#, they expect to get the result as 99991234 but get the result 9999123.	7.2.1.0	7.2.1.0, 7.2.2.0, 7.2.3.0
EXPPORTAL-3058	CCXML Loop count question prop to 7.2.3		7.2.1.0	7.2.3.0
EXPPORTAL-3074	Fetch timeout does not work as expected		7.2.1.0	7.2.3.0
EXPPORTAL-3077	Google Dialogflow does not connect when MPP configured with http/https proxy	If MPP is configured with http/https proxy, then Google dialogflow does not use proxy and fails to connect with error in EndPointMgr.log	7.2.3.0	7.2.3.0
EXPPORTAL-3081	ProcessDocument returned error code -57 during recognition		7.2.2.0	7.2.2.0 7.2.3.0
EXPPORTAL-3061	Transcriptions show DTMF or Speech incorrectly		7.2.2.0	7.2.2.0 7.2.3.0
EXPPORTAL-3086	Dialogflow Setting of language in json payload with followup_event does not switch language for the followup event sent to Dialogflow		7.2.3.0	7.2.3.0
EXPPORTAL-3127	Confidence Threshold not work for DialogFlow		7.2.3.0	7.2.3.0
EXPPORTAL-3130	Dialogflow: Support for play prompt node custom payload		7.2.3.0	7.2.3.0
EXPPORTAL-3164	Make WebLM files in patch "Managed" to allow them to be	Error during patch install.	7.2.3.0	7.2.3.0

ID	Minimum Conditions	Visible symptoms	Release found in	Release fixed in
	quietly ignored if the WebLM app is removed.			
EXPPORTAL-3163	After updating our Aura Experience Portal from version 7.0.2 to 7.2.2 we´re experiencing problems with DTMF recognition, propagation to EP7.2.3		7.2.2.0	7.2.2.0 7.2.3.0
EXPPORTAL-3174	REST API - organizations and zones		7.2.3.0	7.2.3.0
EXPPORTAL-3197	Caller not able to hear TTS responses		7.2.2.0	7.2.2.0 7.2.3.0
EXPPORTAL-3171	ASR input not recognized after media encryption - propagation to 7.2.3		7.2.2.0	7.2.3.0
EXPPORTAL-3195	vb exception cause call drop prop to 7.2.3		7.2.2.0	7.2.3.0
EXPPORTAL-3209	Java java.lang.OutOfMemoryError exception due to org.postgresql.jdbc.PgConnection instances cached in memory	See PSN005488u	7.2.2.0	7.2.0.0 7.2.1.0 7.2.2.0 7.2.3.0
EXPPORTAL-3215	MM Core dump while brigetransfer - prop to 7.2.3		7.2.2.0	7.2.3.0
EXPPORTAL-3223	Unable to forward email to an OD app if the email was generated by another OD app		7.2.2.0	7.2.2.0 7.2.3.0
EXPPORTAL-3231	Change ownership of extracted tar files on patch install.	Leaves files on system as user ID 6006	7.2.1.0	7.2.1.0 7.2.2.0 7.2.3.0
EXPPORTAL-3312	Update USER timestamp for LDAP users as well to trigger user synchronization by POM		7.2.0.0	7.2.0.0 7.2.1.0 7.2.2.0 7.2.3.0
EXPPORTAL-3353	Nuance Greek voice Alexandros incorrectly displayed as F (female) instead of M (male)		7.2.2.0	7.2.2.0 7.2.3.0
EXPPORTAL-3319	Media Manager coredump on G729A codec (propagation)		7.2.1.0	7.2.1.0 7.2.2.0

ID	Minimum Conditions	Visible symptoms	Release found in	Release fixed in
				7.2.3.0
EXPPORTAL-3330	Prop Event handler does not start after Fetch timeout is reached		7.2.1.0	7.2.1.0 7.2.2.0 7.2.3.0
EXPPORTAL-3392	G729 Discontinuous Transmission does not work correctly		7.2.1.0	7.2.1.0 7.2.2.0 7.2.3.0
EXPPORTAL-3404	No immediate progressing after single DTMF digit		7.2.2.0	7.2.2.0 7.2.3.0
EXPPORTAL-3077	Google Dialogflow does not connect when MPP configured with http/https proxy		7.2.3.0	7.2.3.0
EXPPORTAL-3086	Dialogflow Setting of language with followup_event does not switch language for the followup event sent to Dialogflow		7.2.3.0	7.2.3.0
EXPPORTAL-3256	Dialogflow: Remove check for confidence level for Dialogflow		7.2.3.0	7.2.3.0
EXPPORTAL-3265	Dialogflow: def_dialogflow.vxml does not return ResponseArray to parent CCXML session		7.2.3.0	7.2.3.0
EXPPORTAL-3323	Add handling to default vxml app for receiving empty response from Google		7.2.3.0	7.2.3.0
EXPPORTAL-3332	Dialogflow: Change NO_INPUT event name to DF_SYSTEM_NO_INPUT		7.2.3.0	7.2.3.0
EXPPORTAL-3379	Dialogflow - poor performance in gRPC async functions		7.2.3.0	7.2.3.0
EXPPORTAL-3393	Dialogflow: DTMF still visible in MPP logs after setting vxml private property to true		7.2.3.0	7.2.3.0
EXPPORTAL-3398	Dialogflow: Hangup event not sent if far end disconnect during the playing of non-barge-in prompt		7.2.3.0	7.2.3.0
EXPPORTAL-3464	Starting MPP when started results in mpp error state		7.2.3.0	7.2.3.0

ID	Minimum Conditions	Visible symptoms	Release found in	Release fixed in
EXPPORTAL-3465	Increase number of grpc channels from 2 to 12 to decrease call loss during Google outage		7.2.3.0	7.2.3.0

Known issues and workarounds

Installation Issues

ID	Minimum conditions	Visible symptoms	Workaround
EXPPORTAL -1755	If AAEP is upgraded after POM install/upgrade, the soft links get broken	EPM fails to start completely due to broken soft links.	Execute the script "$POM_HOME/bin/vpUpgrade.sh" as root after the AAEP is upgraded to fix the POM soft links.

EXPPORTAL -1434	Upgrading auxiliary EPM from older versions of Experience Portal	The following warning message may appear on some auxiliary EPM upgrades when using autoupgradevp to upgrade from older versions of Experience Portal:
		`Starting automatic upgrade for Experience Portal software. This will take several minutes to complete. Please wait...`
		`-- Initializing install`
		`-- Checking prerequisites`
		`-- Installing prerequisites. Depending on the amount of data being upgraded, this process could take over an hour. IMPORTANT: DO NOT ABORT THE INSTALLATION.`
		`-- Gathering install data`
		`Unable to find configuration file - config/voiceportal.properties(Current directory:/mnt/share/disk1/.`
		`-- Starting install. Please be patient and wait for the Post Installation Summary to be displayed`
		This message can be safely ignored and will be addressed in a future release.
			None required

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”	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 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.
			
			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

ID	Minimum conditions	Visible symptoms	Workaround
			<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 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	Upgrading Experience Portal Primary or Auxiliary EPM on	Installer displays the error "Starting httpd: Syntax error on line 95 of /etc/httpd/conf.d/ssl.conf:	To work around this issue, upgrade the Apache (httpd) package. The minimum Apache (httpd)

ID	Minimum conditions	Visible symptoms	Workaround
	a system with older version of Apache (httpd)	SSLProtocol: Illegal protocol 'TLSv1.1'"	package which supports disabling TLS 1.0 and TLS 1.1 is httpd-2.2.15-54.el6_8.x86_64
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. 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 -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.

ID	Minimum conditions	Visible symptoms	Workaround
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.
EXPPORTAL -645	EPM fails to install when the hostname contains a period	Installing Experience Portal on a server that has a ".' (period) in the hostname will cause the installation to fail. The prerequisite checker fails to detect this condition and allows the install to continue and eventually fail.	Rename the server to remove the period form the hostname.
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**."

Avaya Linux Issues

ID	Minimum conditions	Visible symptoms	Workaround
N/A	Old versions of PuTTY cannot connect	The security hardening done in Avaya Linux result in older versions of PuTTY (e.g. 0.58) not being able to make SSH connections.	Newer versions of PuTTY (e.g. 0.69) work without issue.
N/A	Nonstandard Ethernet configurations	The Experience Portal Avaya Linux upgrade process is expecting the following Ethernet configuration: 1) Eth0 is the primary interface and should have a valid IP and is the network with the default route. This port should not utilize any special configuration like bonding or tagging. 2) Eth1 is the network used with the technicians' laptop and a crossover cable for headless installs.	If this is not the case the system will need to be returned to this state prior to upgrade, otherwise the upgraded system may not have proper network access until the local console is used to repair the network configuration. After the server is upgraded, the Ethernet configuration can be restored to the site specific configuration.

ID	Minimum conditions	Visible symptoms	Workaround
PSN004984u	Dell R630 Ethernet Ports	Dell R630 the Ethernet connections during Headless installs are not as expected.	Follow the information in the following PSN: http://support.avaya.com/css/P8/documents/101038016

OVA Deployment Issues

ID	Minimum conditions	Visible symptoms	Workaround
N/A	Deployment of OVAs on VMWare 6.5	Deployments of Experience Portal OVAs on VMWare 6.5 have been observed with the following behavior: • vCenter-based deployments: The Experience Portal properties that are queried are displayed in a different order than they normally are. This is cosmetic and has no effect on the deployment itself. • ESXi-direct deployments: The deployment wizard may query for Experience Portal properties like a typical vCenter-based deployment would, but any entered values are ignored by VMWare during deployment. Upon bootup of the deployed VM, the startup process will query for Experience Portal properties via CLI as other ESXi-direct deployments normally would.	None required

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	To fix time zone related display issues, update each Experience Portal server to the latest version of

ID	Minimum conditions	Visible symptoms	Workaround
		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.	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 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-1273	MSSQL SQL upgrade script: MSSQL_New_Columns_72.sql	#1, If running the script in batch mode, the script might stop to execute rest of commands if run into some error. #2, Might see the following warning message when the script executes “ALTER TABLE VPAppLog ADD CONSTRAINT VPAPPLOGT1 PRIMARY KEY (VPID, SessionID, MsgTimestamp, SessionIndex, LogType);”: Warning! The maximum key length is 900 bytes. The index 'VPAPPLOGT1' has maximum length of 1040 bytes. For some	#1. Run each SQL command in the script manually at a time. Ignore warning if the comment in the script stated to ignore. #2, It is safely to ignore the warning message of “Warning! The maximum key length is 900 bytes. The index 'VPAPPLOGT1' has maximum length of 1040 bytes. For some combination of large values, the insert/update operation will fail.”

ID	Minimum conditions	Visible symptoms	Workaround
		combination of large values, the insert/update operation will fail.	
EXPPORTAL-1384	Nuance TTS servers and an application with TTS vendor parameters configured.	TTS prompts fail to play through either MRCPv1 or MRCPv2.	Configure Nuance TTS servers for MRCPv2 only and move the TTS vendor parameters in a custom Session XML file instead.
EXPPORTAL-1432	Lumenvox TTS with <say-as> for nospace	Space character added to TTS playback element <say-as>	If the Lumenvox TTS is being used and would like to have no space before the data on <say-as> as shown in the example `<say-as interpret-as="spell”>7</say-as>` the mppconfig.xml needs to be updated by performing the following steps: 1. Log into the MPP as a user with root privileges. 2. Take a backup of the existing $AVAYA_MPP_HOME/config/mpconfig.xml file. 3. Edit the $AVAYA_MPP_HOME/config/mpconfig.xml file and add the xml parameter tag. <parameter name="client.prompt.sayas.nospace">true</parameter> within the <mppsysconfig> and </mppsysconfig> tags. 4. Restart the MPP service. Here is an example: <?xml version="1.0" encoding="utf-8"?> <mppsysconfig> …… <parameter name="PerPort">true</parameter>

ID	Minimum conditions	Visible symptoms	Workaround
			<parameter name="vpms.watchdog">30</parameter> <parameter name="client.prompt.sayas.nospace">true</parameter> .... </mppsysconfig>
EXPPORTAL-1510	Upgrade Primary EPM with a configured HTTP connection	The "Type" field for the existing HTTP connection (outbound) shows empty in View HTTP connections page after upgrading EP (7.1 to 7.2)	Go to the Change HTTP Connection and click on the Save button. Note: Even though the Type is empty, the HTTP Connection is still considered and used as an Outbound HTTP Connection.
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-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-3351	Using Google Dialogflow	Intermittent and infrequent freeze seen in MPP, can last up to 4 minutes but recovers automatically. Can impact non Dialogflow calls also. 5 freezes noticed during 72 hour traffic run @15kcph, 450 concurrent calls.	Limit the number of concurrent voice calls to Google Dialogflow to less than 150 per MPP
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 Dialoglfow, 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.

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

Documentation errata

Document number	Title	Description

Contacting support

Contact Support Checklist

Refer to the Avaya Aura® Experience Portal 7.2 Documentation Library for the Troubleshooting section. Or the Avaya Technical Support Web site https://support.avaya.com and the document titled "**Troubleshooting Avaya Aura® Experience Portal**" (*https://downloads.avaya.com/css/P8/documents/101039767*).

If you are having trouble with Avaya Aura® 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.