Avaya Experience Portal Overview and Specification

Release 8.1.2.3
Issue 1
August 2025

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 media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

“**Hosted Service**” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

The Global Software License Terms (“Software License Terms”) are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

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, 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

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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

Chapter 1: Introduction

Purpose

This document describes tested Avaya Experience Portal characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security, and licensing requirements.

This document is intended for people who want to gain a high-level understanding of the Experience Portal features, functions, capacities, and limitations.

New in this release

Avaya Experience Portal R 8.1.2 Service Pack 3 includes the following changes:

Platform Updates

Experience Portal platform has undergone significant upgrades to enhance performance, stability, and security:

- **JDK**: Upgraded to Azul Zulu OpenJDK 17.0.14 for enhanced security and LTS support.

Security Updates

New security measures for Experience Portal are:

- **Apache Tomcat**: Upgraded to 9.0.106 to resolve the security vulnerability - CVE-2025-31651. Improper Neutralization of Escape, Meta, or Control Sequences vulnerability in Apache Tomcat.
- **PostgreSQL**: Upgraded to 17.4 to resolve below security vulnerabilities:
    - CVE-2024-10979 - Incorrect control of environment variables in PostgreSQL PL/Perl
    - CVE-2024-10977 - PostgreSQL libpq retains an error message from man-in-the-middle
- **ActiveMQ**: Upgraded to 6.1.6 to resolve below security vulnerabilities:
    - CVE-2024-38819: Spring Framework functional endpoints vulnerable to path traversal allowing file access.
    - CVE-2022-22970: DoS vulnerability in Spring due to multipart file upload data binding.
    - CVE-2022-22971: DoS issue in Spring multipart handling like CVE-2022-22970.
    - CVE-2022-22950: DoS via crafted Spring Expression Language (SpEL) expressions.

- **Content-Security-Policy (CSP) headers**: Added Content-Security-Policy headers in AEP with unsafe inline option for stronger protection against cross-site scripting (XSS) and code injection attacks.
- **X-XSS-Protection header**: Disabled the X-XSS-Protection header, as Content-Security-Policy (CSP) now provides a more robust and modern alternative.
- **Missing role-based access restrictions**: Added Missing-role-based access restrictions to Experience Portal for proper permission enforcement upon user role changes.
- **TLS v1.3**: Supported for secure communication across key components such as Primary/Aux EPM, MPP, Application Server, Avaya SM, ASR/TTS Speech Server, Nuance and Google cloud servers, and POM.
- **SRTP sips Requirement Update**: The mandatory sips requirement for SRTP (Secure Real-time Transport Protocol) is removed and is now a configurable option. SRTP encryption headings can be added if URI Scheme is set to SIP and TEL.

Vulnerability Remediation

Addressed critical vulnerabilities identified through Coverity and Black Duck scans.

For changes in previous releases, see Changes in earlier releases on page 8.

Changes in earlier releases

Avaya Experience PortalR.8.1.2 SP2

Avaya Experience Portal R 8.1.2 Service Pack 2 includes the following changes:

Google Dialogflow - support of reverse proxy

Experience Portal supports the configuration of reverse proxy for Google Dialogflow.

MPP port utilization alerts or alarms

Experience Portal supports real-time alerts through alarms and a Simple Network Management Protocol (SNMP) trap. The following events are generated when Media Processing Platform (MPP) port usage exceeds a certain percentage of capacity.

- New log Event PSYSM00059 is generated when the MPP port use exceeds the configured high threshold.
- New log Event PSYSM00060 is generated when the MPP port use exceeds the configured low threshold.
- New log Event PSYSM00061 is generated when the MPP port use falls below the configured low threshold.

Ability to select default speech engine for ASR

Experience Portal supports enabling default Automatic Speech Recognition (ASR) selection when multiple ASRs are assigned to the application.

NuanceMix DLGaaS - ability to request different dialog or bot from the same OD or VXML application

Experience Portal supports Nuance Mix Dialog as a service to call multiple dialogs or bots within the same call.

Capability to export reports in .csv format

Experience Portal supports exporting standard, custom EP, and POM reports in `.csv` format.

Capability to reset application cache using webservice

Experience Portal supports resetting the MPP application cache through a webservice.

Audit log or Alarms log functionality refinement

Experience Portal supports enhanced audit, alarm logging, optimized queuing logic, and improved database connection pooling to improve performance and ensure that log entries are processed efficiently.

New legal name in software and documentation

Avaya LLC is the company's new legal name. All instances of Avaya Inc in the documentation and software are updated to Avaya LLC. This includes names on the User Interface, all Linux files, and scripts.

Platform upgrades:

- Upgraded Apache Tomcat to 9.0.89.
- Upgraded embedded Postgres to 16.03.
- Upgraded RHEL 8.10 for bare metal and OVA in line with Aura.

Security upgrades:

- Added security headers in Avaya Experience Portal.
- Updated third-party libraries to address various security vulnerabilities.
- Disabled support for static key ciphers.
- Disabled support of cryptographically weak hash-based message authentication codes (HMACs).
- Remediated Qualys, Coverity, and Blackduck critical issues.

Avaya Experience Portal R8.1.2 SP1

Avaya Experience Portal R8.1.2.1 includes the following new capabilities:

- **Enhancements:**
- - Added option to configure the nuance mix domains other than nuance.com.
  - Removed support for deprecated *interactive_voice_response_settings* variable for googleapi v3alpha1.
- **Platform:**
  - Support for OpenJDK 17.0.7 Java LTS for external app server (for OD runtime) and OD dev workstation.
  - AEP SW only support of RHEL 8.5, 8.6, 8.7 & 8.8 versions.

- **Security:**
    - Support for OAuth 2.0 connections to IMAP and SMTP servers.
    - Added missing role based restrictions in experience portal.
    - Patches updated to address security vulnerabilities.

Avaya Experience Portal R8.1.2

Avaya Experience Portal R8.1.2 includes the following new capabilities:

- Google CCAI Dialogflow enhancements:
    - Enhanced selection of Dialogflow v3 Projects and Agents
    - Enhanced sample app for Voice, Mobile, Chat, and SMS with Google Dialogflow
    - Default Dialogflow VXML to use the StreamingAnalyzeContent method for events
- Certificate enhancements:
    - WebLM utilizing AEP Certificate Architecture
- Security enhancements:
    - Logging updated from log4j to log4j2
- Support for RHEL 8.4
- Third-party software versions updated to latest release

Avaya Experience Portal R8.1.1

Avaya Experience Portal R8.1.1 included the following new capabilities:

- Dialogflow enhancements:
    - Support for licensing distribution to align with ASR model
    - VAD selection to support selection of local or remote VADs
    - Support for receiving and processing partial responses via streaming API
- Support for Nuance Mix DLGaaS full native integration:
    - With Avaya Experience Portal Nuance Mix DLGaaS integration, customers can access Cloud AI based automation for voice calls through Experience Portal.
- Enhanced vendor-specific speech license distribution that supports skipping a zone that does not have any speech servers using that license.
- Support to enable/disable SSH service for EASG CLI login on AEP running on ASP 130 R5.
- Support to modify LDAP Session configuration via webservice.
- Support for outbound performance enhancement with MPP to cache ccxml content.
- Support for default umask of 0027.
- PostgreSQL upgrade to 12.8.
- Tomcat upgrade to 8.5.72.

Avaya Experience Portal R8.1

Avaya Experience Portal R8.1 included the following new capabilities:

- Support for Voice Activity Detector (VAD) Package.
- Support for auto-upgrades from release 6.x to 8.x.
- Support for VMware 7.x.
- Support for enhanced password complexity in the AEP installer.
- Support for PostgreSQL 12.6.
- Support for Tomcat 8.5.64.
- Support for Pale Moon browsers.
- Support for Speech Usage Metering.
- Support for Security Enhanced Linux (SELinux).
    - SELinux is fully supported in enforcing mode.
- Support for latest AEP third-party software releases.
- Support for Enhanced Alarm Generation.
    - New log event PTELE00044 is generated when the returned error APIs do not contain enough information.
    - New log event PTELE00045 is generated when the client specifies an invalid argument in the API.
    - New log event PTELE00046 is generated when the response for the client request arrives after a timeout.
    - New log event PTELE00047 is generated when the requested resources in the client request is not found in the server-side.
    - New log event PTELE00048 is generated when the entity that a client attempted to create already exists.
    - New log event PTELE00049 is generated when the client does not have permission to execute the specified operation.
    - New log event PTELE00050 is generated when the client requested resource is exhausted.
    - New log event PTELE00051 is generated when the operation was rejected because the system is not in a state required for the operation's execution.
    - New log event PTELE00052 is generated when the operation was aborted, typically due to a concurrency issue.
    - New log event PTELE00053 is generated when the operation was attempted past the valid range.
    - New log event PTELE00054 is generated when the operation is not implemented or supported/enabled in this service.
    - New log event PTELE00055 is generated when some infrastructure expected by the underlying system has been faulty. This error code is generated for serious errors.

  - New log event PTELE00056 is generated when the requested service is currently unavailable.
  - New log event PTELE00057 is generated when unrecoverable data loss or corruption occurs.
  - New log event PTELE00058 is generated when the client request contains invalid authentication credentials for the service.
- Support for third-party TTS and ASR speech servers.
- Improved Dialogflow config screens.
- Support for uploading identity certificates for EPM and MPP through the EPM web interface
- Support for deploying Avaya Experience Portal on the following customer - hosted platforms:
  - Deploying Avaya Experience Portal on Amazon Web Services.
  - Deploying Avaya Experience Portal on Google Cloud Platform.
  - Deploying Avaya Experience Portal on Microsoft Azure.

Avaya Experience Portal R8.0

Avaya Experience Portal 8.0 included the following new capabilities:

- Change of brand name from Avaya Aura® Experience Portal to Avaya Experience Portal.
- Support for RedHat 8.x Operating System: To be used for configurations where Avaya provides the Operating System (hardware platform or OVA).
- Support for RedHat 7.x and 8.x for customer provided RHEL.
- Support for additional FIPS compliance enhancements in EPM, MPP, and third-party applications:
  - Certificates Import updates and VPAppIntfClient updates for FIPS mode
  - New PADMN0009 log event when EPM has started and FIPS is enabled on the system
- Support for Internet Protocol version 6 (IPv6).
- Experience Portal to limit the number of concurrent sessions per user and limit the total number of concurrent sessions.
- Ability for administrative accounts to configure a password policy for programmatic access.
- Support for Experience Portal to be deployed using Docker containers.
- Support for small, medium, and large OVA profile options to allow sites to configure system resources for lower than maximum capacity.
- Support for upgrades from Avaya CSR2, CSR3 (HP DL360 G9, Dell R630), ACP110, and ACP130.

  For more information on ASP platforms, see the *Avaya Converged Platform Overview and specification* guide on the Avaya Support website at http://support.avaya.com.
- Support for the new PLDS license version that includes all the current licenses for the third-party components.
- Support for Experience Portal to count and enforce MRCP, ASR, and TTS proxy licenses.

- Support for upgrades from Experience Portal version 7.x.
- Support for latest versions of third-party applications including Tomcat, Postgres, Apache HTTP, and SpiderMonkey.
- Support for the latest versions of browsers such as Chrome, Firefox, Internet Explorer, Safari, and Microsoft Edge.
- Updated AAEP/POM sizing tool to include the new OVA profiles and other AAEP server/OVA sizing impacts.
- Support for providing reports in xlsx format.
- Support for the security certificate re-architecture.
- Included two new certificate tabs in the Certificates page: EPM Identity Certificate and MPP Identity Certificate.
- Included three new certificate expiration alarms: PCERT02511, PCERT02512, PCERT02513, and PCERT02514.
- Support secure syslog communication to external syslog servers.
- Included three new EASG alarms for PEASG events: PEASG02501, PEASG02502, and PEASG02503.
- Included two new licensing alarms: PLICE00027 & PLICE00028.
- Updated www.zang.io to cloud.zang.io to support the new location of the Zang dashboard.
- Support for MariaDB JDBC Driver class.

Avaya Experience Portal R7.2.3

The following new capabilities were added in Avaya Experience Portal R7.2.3:

- Support for Google Dialogflow full native integration: With Avaya Experience Portal Google Dialogflow integration, customers can access Cloud AI based automation for voice calls through Experience Portal.
- Support for a Call Anchoring license.
- Support for Google Dialogflow Connections license.
- Support for Google Dialogflow ASR Server.
- Support for Google Dialogflow for Applications.
- FIPS 140-2 compliance: Experience Portal now supports the ability to enable or disable the use of FIPS 140-2 compliant modules or ciphers.
- Support for PostgreSQL 11.4.
- Support for Tomcat 8.5.42.
- New log event PSESM00095 for the license enforcement feature for Google Speech and Google DialogFlow.
- New log event PTELE00043 for when the stream Media Manager and Google shuts down unexpectedly.
- Support for the new and more secure password hashing algorithm SCRAM-SHA-256 for database users.

- Ability to use certificate-based authentication for the VPAppLogClient and VPAppLog web service.
- Support for key rotation on DialogFlow and Google Speech - Cloud ASR customers can rotate credentials using a new REST API.

Avaya Experience Portal R7.2.2

The following new capabilities were added in Avaya Experience Portal R7.2.2:

- Support for Nuance Speech Suite 11
    - Support for Nuance 11.0.2 (Recognizer 11, Vocalizer 7).
    - Support for the new Nuance Dragon Voice — Only for VXML applications.
        - For more information on this feature, see the Nuance documentation.
- Support for Avaya Ava SMS
    - Avaya Ava can now receive and reply to SMS messages: Experience Portal can forward an SMS to Avaya Ava, and Ava can then send a response back using Experience Portal SMS resources.
    - Experience Portal can now generate reports on Avaya Ava SMS support usage.
- Support for inbound and outbound MMS in the Avaya OneCloud CPaaS connector using Avaya OneCloud CPaaS Communication APIs for SMS integrations.
- Support for outbound SMS for provider i2SMS.
- Support for VoiceXML applications to delay acquisition and early release of speech resources.
- Support for new CCXML hint `<join/>`.
    - Experience Portal can clamp or block DTMF in one direction only.
- Support for native integration to Google Speech. Experience Portal now enables the use of Google Speech as an ASR provider.
    - The Add and Change ASR Server pages have new fields that are specific to Google Speech Engine Type : Credentials, Profanity Filter, and Audio Chunk Size.
- Support for the following latest versions:
    - Tomcat 8.5.33
    - Postgres 10.1
    - Jasper reports 6.6
- Support for the new common server ACP 110 (bare-metal) and ACP 130 (VMWare).
- Support for two new GDPR (General Data Protection Regulation) related database scripts.
- Support to use multiple speech recognition vendors on a call.
- New counted license for Google ASR Connections.
- Users can now set speech vendor specific parameters in Voice XML applications.
- Identifying Nuance call logs with the ASR application that is running on Experience Portal.
- New log event PSESM00093 for the multiple vendor feature. This event identifies when MPP cannot load a grammar if the speech vendor was not specified or valid.

- New log event PSESM00094 for MPP JSON parsing errors.
- Support for Google Speech as a speech recognition engine.

Avaya Experience Portal R7.2.1

The following new capabilities were added in Avaya Experience Portal R7.2.1

- Support for new HTTP Connectors:
    - AT&T Landline Texting
    - Zipwhip
- Email Destination groups support:
    - Six predefined Email Destination groups.
    - Ability to change the display name of the email destination groups.
    - Adding one more email address to an Email Destination Group.
    - Specifying of one or more email groups per alarm.
    - Ability to specify additional or custom email text per alarm to be sent with the alarm email notification.
- New Authentication protocol and Privacy protocol added to SNMP Agent settings Version 3 group.
- Support for additional Application Alarms Code ranges for Orchestration Designer applications:
    - Alarm Offset CAV is included as part of the Alarm Offset PDC that allows the administrator to define the offset to be used for the generating the range of alarms.
    - Nine additional critical alarms - QAPP_000[1-9]3
    - Nine additional major alarms - QAPP_000[1-9]2
    - Nine additional minor alarms - QAPP_000[1-9]1
- Support for Server name indication (SNI) in VoiceXML and CCXML browsers.
- Reporting Enhancements:
    - SMS Lookup:
        - The existing Media Type filter on the Contact Summary and Contact Detail filter pages includes SMS Lookup.
        - Two additional entries added to Contact Summary Report (Summary By SMS Statistics table):
            - Number of SMS Lookups
            - Number of Failed SMS Lookups
    - Summary by DNIS:
        - The Contact Summary filter page displays DNIS added to the Summarize By list box.
        - A new table is generated in the Contact Summary Report listing each DNIS and the associated total minutes used, peak busy ports, and number of contacts.

- Integration with the Avaya Breeze® platformsystem to allow the usage of EPSMS resources for two way SMS.
- Support for long polling for Avaya Zang:
  - Configuration changes are required in the Zang admin console.

Avaya Experience Portal R7.2

The following new capabilities were added in Avaya Experience Portal R7.2:

- SMS support
  - Integration of Avaya Zang as a new HTTP connector
  - Configure the connection type to be either incoming/outgoing or outgoing
  - Add the SMS gateway to support the SMPP connections over TLS 1.2
  - Add the EPM configuration to support the SMPP connections over TLS 1.2
- Avaya Experience Portal Reporting support
  - Offer a subscription 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
  - Reset the SessionIndex value on each new SessionId inside the AppLog Web Service to prevent duplicate records under certain error conditions
  - Include the moduleidnodeid item in the “Message” details view when drilling into an Application Log (VPApplog) entry
- Early media support
  - Ability for administrators to configure the early media though the EPM web interface for application types that include voice, including VoiceXML, CCXML, or VoiceXML/CCXML
  - Application support to indicate whether the administrator has enabled early media or not for that application during an inbound call when Avaya Experience Portal launches an application
  - Early Media Reporting support
- RFC 4240 implementation support
  - Implement RFC 4240, Basic Network Media Services with SIP
  - Ability for administrators to configure the pre-installed RFC 4240 CCXML application through the EPM web interface
- Speech Server utterances support
  - Ability for administrators to enable the Speech Server utterance recording on a per application basis through the EPM web interface
  - Provide the application to obtain the URL of the recognized utterance after issuing a speech recognition request
- Application Specific Speech parameters for administrators for Session XML support
  - Specify that a Nuance speech server (ASR & TTS) that is configured through the EPM web interface to use MRCPv2 to support the session.xml parameter

  - Specify the session.xml parameters that an application must use for ASR through the EPM web interface
  - Specify the session.xml parameters that an application must use for TTS through the EPM web interface
- MPP alert status support
  - Support to alerts that MPP is shutting down alert all CCXML applications registered for a shutdown event.
- Selecting Speech Languages and Voices support for listing all
  - Selected ASR languages in a list, separate from the list of all installed ASR languages in the EPM web page.
  - Selected TTS voices in a list, separate from the list of all installed TTS voices in the EPM web page.
  - Installed ASR languages in a list, separate from the list of all possible ASR languages.
  - Installed TTS voices in a list, separate from the list of all possible TTS voices.
- Global configurable application variables support
  - Ability for administrators to configure the user defined global configurable application variables. These variables are system wide variables that are not specific to any particular application or zone specific.
- Codecs support
  - Offer the supported codecs, such as G.711, G.729 in a priority order that is configurable by administrators when sending a SIP INVITE.
  - Accept the supported codec, such as G.711, 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.
- Avaya Breeze® platform integration support
  - The EPM User Interface is updated to use Avaya Breeze® platform instead of Engagement Development Platform.
- Avaya Experience Portal security improvement 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.
  - For administrators to download CSR.
  - For administrators to upload signed certificate that is based on the CSR generated by the system.
  - For the EPM web interface to provide certificate based authentication as an alternative to requiring the user to enter a user name and password.
  - 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 support for the Avaya Experience Portal system to address security vulnerabilities in prior TLS versions.

    - For validating the server certificate identity.
    - For administrators to enable or disable the server identity validation. The default for freshly installed systems shall be to enable identity validation.
- Enhanced Access Security Gateway (EASG) support
    - For Avaya Experience Portal to use EASG for the authentication of all supported Avaya Services logins
    - For EASG Avaya Service Login names limited to, init, inads, craft, and sroot
    - For EASG Avaya Services Login Interface
- New common server
    - Dell R630 common server support

Avaya Experience Portal R7.1

The following new capabilities were added in Avaya Experience Portal 7.1:

- Mobile Web Support
    - Support for HTML applications created using Orchestration Designer.
    - Support for configuration of HTML application.
    - Support for HTML applications to be associated with a zone and with an organization.
    - Support for HTML status and usage in Real-time Monitoring.
    - Support for HTML in Maintenance Reports.
    - Support for HTML application type in Historical Reports.
    - Support for HTML application type in Management Web Services.
- Conversations
    - Support for cross-channel conversations.
- Licensing
    - New licensed features
        - HTML Units.
    - Enforcement
        - System wide enforcement on a daily basis.
        - Each HTML unit allows one HTML application launch per day.
    - Fresh install
        - Can use HTML during initial 30 day grace period.
    - License Server
        - Ships with WebLM 7.0.
- Contact Center Integration
    - Support to associate Avaya Breeze® platform with Experience Portal.

  - Support for storing conversation data of non-SMS applications.
- Single Sign-on through System Manager Integration
  - Support for a minimal level of integration with System Manager to provide single sign-on from System Manager to Experience Portal.
- EPM user accounts
  - Support for indefinite locking of user accounts.
  - Support for configurable user locked out message.
- Configurable Application Variables
  - Support for confirmation for deletion of a configuration application variable file.
- Reports
  - Support for a Trending by option from the Contact Summary (Filters) page.
- Third party certificates
  - Support for Primary EPM, Auxiliary EPM, MPP and Single server third-party signed security certificates.
- Upgrades
  - For non-OVA based systems: Support for upgrade of systems running Experience Portal 6.0 or later.
  - For OVA based systems: Support for upgrade of systems running Experience Portal 6.0 SP2 or later.

Avaya Experience Portal R7.0.1

The following new capabilities were added in Avaya Experience Portal R7.0.1:

- The certificate generation code is enhanced to use a more secure hashing algorithm.
  - All security certificates generated by Experience Portal now use the SHA-256 algorithm with a 2048 bit key
  - New scripts for replacing server certificate outside of install:
    - GenerateServerCertificate.sh to generate a new self-signed certificate
    - ImportServerCertificate.sh to import a customer provided certificate
  - The ability to generate or upload a new root certificate from the **Security** > **Certificate** > **Root Certificate tab** of EPM
- Support for Nuance Vocalizer 6.0 as speech server.
- Management Interface web service to allow client applications to manage Experience Portal applications and configurable application variables.
- Support for MySQL as an external database.
- Support for single server Experience Portal systems deployed in the Avaya Customer Experience Virtualized Environment.

- SMS
  - Support for conversations
  - New utility TestSMPPConnection
  - Support for service provider AOS
- Email
  - Launch application by cc
  - Launch application by user name
  - Support for STARTTLS transport
- VoiceXML/CCXML
  - Pass termination reason from CCXML to VoiceXML
- Speech
  - Support for multiple instances of Nuance on a single server
- Licensing
  - Can now use ASR, TTS, email, SMS, and zones during initial 30 day grace period

Avaya Experience Portal R7.0

The following new capabilities were added in Avaya Experience Portal R7.0:

- Allocate resources and ports as per zones
  - Create and administer zones
  - Allocate resources such as Auxiliary EPM servers, MPPs, Speech Servers, VoIP Connections (H.323 and SIP), Applications, SMS, email, and so on to the zones
  - Allocate ports to zones
  - Add organizations to the zones
- Multi-channel support
  - Support for email and SMS as additional communication channels
  - Two-way text-based self-service application support: person-to-application and application-to-person
  - Multichannel application development/runtime framework (Orchestration Designer)
  - Web services and connectors for SMS and email notification
  - Capability to configure multiple email processors and SMS processors for inbound and outbound messages
  - Support cross channel inbound and outbound messages. For example, triggering an outbound email as a result of an inbound SMS
- New licensed features
  - Email units
  - SMS units

  - Zones
- New reports to support the new media types, SMS and Email. The data for generating these reports is added to the existing CDR and SDR.
- Ability to install and upgrade Experience Portal in the Avaya Customer Experience Virtualized Environment. The Experience Portal virtualized environment offer consists of the following three OVA files:
  - Primary EPM
  - Auxiliary EPM
  - MPP

Chapter 2: Overview

Experience Portal overview

Avaya Experience Portal provides a single platform for automated voice and multimedia, self-service, and Interactive Voice Response applications. Experience Portal supports inbound and outbound calls, Short Messaging Service (SMS), email, and HTML applications.

Experience Portal supports Session Initiation Protocol, H.323, and a mixed telephony environment.

For self-service, use the following features of Experience Portal:

- Intelligent Customer Routing: For enhanced wait treatment and load balancing.
- Proactive Outreach Manager: For outbound calls, email, and SMS campaigns.

Configuration options

You can install Experience Portal on a single or multiple servers, depending on the number of telephony ports required.

- The single server configuration includes a single server running the Experience Portal Manager (EPM) and Media Processing Platform (MPP) software.

  You can deploy the single server configuration with an optional co-resident application server.
- The multiple server configuration includes two or more servers:
  - One server for the primary EPM software
  - Minimum one server for the MPP software to handle inbound and outbound calls

    You can also deploy an auxiliary EPM server to handle failover for Application Interface web service requests.

    SMS, email, and HTML processors can be hosted on a primary or auxiliary EPM.

Feature description

Avaya Experience Portal provides the following software elements:

- Media server software: To provide IVR-based functionality and call classification.

- Experience Portal Manager (EPM) and Auxiliary EPM applications:
    - To provide centralized management and support for Experience Portal and its features, Proactive Outreach Manager, and Intelligent Customer Routing.
    - To provide SMS, email, and HTML channels.
- Web Server host: To provide the standards-based VoiceXML, CCXML, or TextXML script to the media server. Web Server also hosts email and HTML applications as required for smaller deployments. Larger deployments support customer-provided application servers.
- Avaya Orchestration Designer tool: To build speech, call control, and message applications. You can deploy the VXML or CCXML applications on an existing Apache Tomcat, IBM WebSphere, Oracle WebLogic, or JBOSS Web server environment. You can also deploy TextXML-based applications that are developed with Orchestration Designer.
- Orchestration Designer: To support application development for Experience Portal.

Related links

Avaya Experience Portal media servers on page 23
Experience Portal Manager on page 23
Application execution environment on page 28
Multichannel components on page 28
Mobile channel components on page 28
Avaya Orchestration Designer on page 29
Proactive Outreach Manager on page 29
Intelligent Customer Routing on page 29
Call classification on page 30
Zoning on page 30

Avaya Experience Portal media servers

Avaya Experience Portal supports the Media Processing Platform (MPP) media server. Media servers provide the following automation functionalities:

- Terminating telephony sessions.
- Liaising with third-party speech and other multimedia services.
- Managing VoiceXML and CCXML sessions.
- Controlling multiple voice dialogs and sessions.
- Providing advanced call control functions with a programmable CCXML Session Manager.

Media server software integrates with IP Telephony infrastructures through H.323 or SIP and RTSP while managing external speech and media resources.

Related links

Feature description on page 22

Experience Portal Manager

Experience Portal Manager provides a centralized operation, administration, management, and provisioning interface for Experience Portal, Intelligent Customer Routing, Proactive Outreach

Manager, and other Avaya and Avaya Partner applications. It is an easy-to-use web-based interface that provides the following:

- Media servers that support all concurrent self-service sessions across your enterprise, including email, SMS, and HTML.
- VoIP, application, and speech resource provisioning.
- Web service for outbound voice calls.
- Reports that you can customize.
- Failover mechanism in case of loss of a media server.

Related links

Feature description on page 22
Primary EPM and Auxiliary EPM server overview on page 24
Directory details of the EPM system components on page 25
EPM components on page 26

Primary EPM and Auxiliary EPM server overview

All Experience Portal systems with Media Processing Platform (MPP) must have a primary EPM server. In addition, if your system is configured to use dedicated server machines for the EPM and MPP software, the system can also have auxiliary EPM servers that handle outgoing calls when the primary EPM server is unavailable.

Primary EPM server

The EPM software on the primary EPM server:

- Includes the EPM web interface that provides a centralized administration and configuration tool. When a user logs into the EPM web interface, the user role associated with the username dictates which pages the user can see and what actions the user can perform.
- Sends relevant configuration information to each MPP and auxiliary EPM server.
- Routes outgoing calls made with the Application Interface web service to an available MPP server.
- Collects the operational status from each MPP and auxiliary EPM server and displays it on the EPM web interface.
- Monitors the heartbeat of the MPP servers and redistributes telephony ports when an MPP fails.
- Monitors the heartbeat of the auxiliary EPM servers and redistributes relevant resources when an auxiliary EPM fails.
- Receives event and alarm messages from all MPP and auxiliary EPM servers.
- Downloads report data from all MPP and auxiliary servers and stores it in the Experience Portal database so that users can create reports that contain information from all MPP and auxiliary servers in the system.
- Interacts with the Avaya WebLM license server to distribute and manage Automatic Speech Recognition (ASR), Text-to-Speech (TTS), and Telephony ports across all MPP servers.

- Interacts with the Avaya WebLM license server to distribute and manage Email, SMS, and HTML resources across all auxiliary EPM servers.
- Provides an optional Simple Network Management Protocol (SNMP) interface to monitor Experience Portal alerts.
- Handles Application Logging web service requests.
- Handles Management Interface web service requests.
- Handles outbound and inbound email and SMS messages.
- Handles inbound HTML launch requests.

Auxiliary EPM server

The EPM software on the auxiliary EPM server:

- Assigns outgoing calls made with the Application Interface web service to an available MPP server. However, Experience Portal does not provide automatic load balancing or failover. You must use a third-party product for these purposes.
- Shares Application Logging web service requests when the primary EPM server is in service and handles all the application logging requests when the primary EPM is not functional.

  Note:

  When using the Application Logging web service, applications written with Orchestration Designer provide failover and load balancing between the primary and auxiliary EPM servers. Applications written with other tools must provide their own load balancing and failover mechanisms for this web service.
- Handles outbound and inbound email and SMS messages.
- Handles inbound HTML launch requests.
- Does *not* include the EPM web interface; therefore, the Auxiliary EPM server cannot be used to administer the system or monitor the status of the MPP servers.

Related links

Experience Portal Manager on page 23

Directory details of the EPM system components

Most Experience Portal components and log files are located in the default installation directory that you specify during installation. However, several components cannot be relocated and are stored in fixed paths even if you specify a different path than the default installation directory.

The following table lists some of the components that are stored in fixed paths.

This table does not include standard RHEL packages, such as Apache and NTP, that are installed with or used by Experience Portal.

Component	Directory
Experience Portal Manager web application	`/opt/Tomcat/tomcat/webapps/VoicePortal`

Table continues…

Component	Directory
Experience Portal Management web services	`/opt/Tomcat/tomcat/webapps/axis2`
Avaya License Manager	The collocated WebLM is installed in the `/opt/WebLMServer/tomcat/webapps/WebLM` directory. If you use an Standalone WebLM, the license manager can be installed in a different directory on the external system.
Experience Portal database	The Postgres files are installed in the `/var/lib/pgsq`l directory. Most of the database data is in the `/var/lib/pgsql/data` directory.
Tomcat for EPM and HTML	`/opt/Tomcat`
Tomcat for SMS and Email Processor	`/opt/MMSServer`
Apache Axis2: web services container	`/opt/Tomcat/tomcat/webapps/axis2`
Postgres Database	`/var/lib/pgsql`
Experience Portal Backup	`/opt/Avaya/backup`
Install Agent	`/opt/Avaya/InstallAgent`

Core Services	`/opt/coreservices`
	`/opt/Avaya/CoreServiceConfig`
	`/opt/Avaya/CoreServiceInstall`

Related links

Experience Portal Manager on page 23

EPM components

The EPM software, which is installed on the Linux operating system, consists of the following components:

- Experience Portal Manager web application
- Experience Portal web services
- Application Log Manager
- Alarm Manager
- Network Log Manager
- Avaya License Manager
- Experience Portal database
- SMS and Email Processor web application
- HTML web application

The EPM also relies on the following third-party components, which are automatically installed as part of the EPM installation:

- Zulu OpenJDK: Java run-time environment based on OpenJDK distribution
- Apache Tomcat: web servlet container
- Apache Axis2: web services container
- PostgreSQL: SQL database server

Experience Portal Manager web application

The Experience Portal web application serves several purposes, including:

- Provides graphical webpages for configuring and administering the Experience Portal system.
- Sends relevant configuration information to each media server.
- Collects operational status from each media server.
- Collects report data from each media server.
- Collects license information from Avaya License Manager

Application Log Manager

The Application Log Manager receives log entries from the applications developed with Orchestration Designer and writes those entries to the Experience Portal database.

Alarm Manager

The Alarm Manager monitors the entries logged by the Network Log Manager. Alarm Manager also generates an alarm whenever appropriate.

Network Log Manager

The Network Log Manager receives log entries from several Experience Portal components and writes those entries to the Experience Portal database.

Avaya License Manager

Several Avaya products share the Avaya License Manager (WebLM) component. When you purchase Experience Portal, you receive a license file from Avaya that specifies the number of various licensed features that you purchased. For example, Telephony ports, Automatic Speech Recognition (ASR), Text-to-Speech (TTS), Email, HTML, SMS resources and so on. Experience Portal must be able to communicate with the WebLM server to determine the various licensed features that you purchased.

The WebLM server software is automatically installed with the Experience Portal primary EPM software. However, you can also connect your Experience Portal server to a dedicated WebLM server machine, which is shared among all Avaya products.

Experience Portal database

The Experience Portal database stores important Experience Portal data for EPM and the media servers.

The Experience Portal database is located on the Primary EPM server. Hence, you do not need to take backups of the the MPP servers and the auxiliary EPM servers.

Note:

Ensure that you do not not modify the Experience Portal internal database. For assistance about modifying the database, contact your Avaya technical support representative.

Related links

Experience Portal Manager on page 23

Application execution environment

The web server host, such as Apache Tomcat web server, provides the standards-based VoiceXML and CCXML applications to the Experience Portal media servers. You can also use the existing web application servers for application management.

You can deploy Application execution environment in a virtualized environment. This environment reduces the business hardware footprint and lowers the capital and operational expenses.

Related links

Feature description on page 22

Multichannel components

Experience Portal provides the following components to support SMS and email:

- SMS Web Application: An application that provides web user interface for configuring and managing the SMS-related components.
- SMS Processor, SMS Browser, and SMS Web Services: A web application that interacts with an SMSC over the SMPP protocol and sends and receives SMS messages. The web application includes the capability to process inbound SMS messages and supports execution of Orchestration Designer applications for outbound SMS messages.
- Email Web Application: An application that provides web user interface for configuring and managing the email-related components.
- Email Processor, Email Browser, and Email Web Services: A web application that interacts with an email Server over the SMTP and IMAP4 protocol and sends and receives email messages.
- Multi Media Central Web Services: An application that acts as an interface to the external client and sends SMS and email messages.

Related links

Feature description on page 22

Mobile channel components

Avaya Experience Portal provides the following components to support HTML:

- HTML web application: To provide web user interface for configuring HTML-related components.
- Application Interface web service method: To launch HTML applications.

Related links

Feature description on page 22

Avaya Orchestration Designer

Using Orchestration Designer, you can build speech, call control, and message applications and develop HTML applications. You can deploy these VXML or CCXML applications on an existing Apache Tomcat, IBM WebSphere, or Oracle WebLogic web server environment. You can also deploy the textXML applications developed using Orchestration Designer.

In Experience Portal, you must use Orchestration Designer to write SMS and email applications.

Orchestration Designer is available at no added cost with every Experience Portal purchase. You can download it from Avaya DevConnect at http:// www.avaya.com.

✱ **Note:**

Experience Portal supports SMS and email applications developed using Orchestration Designer 7.0 or later.

Experience Portal supports HTML applications developed using Orchestration Designer 7.1 or later.

Related links

Feature description on page 22

Proactive Outreach Manager

Proactive Outreach Manager (POM) is a managed application of Avaya Experience Portal.

POM provides unified, multichannel, inbound, and outbound architecture with the capability to communicate through different interactive channels such as SMS, email, voice, and video.

Related links

Feature description on page 22

Intelligent Customer Routing

Intelligent Customer Routing (ICR) is a managed application that provides features to efficiently handle customer calls.

ICR provides the following features:

- Self-service using Avaya Experience Portal as the first point of access to an organization.
- Intelligent routing of calls to a relevant call center across applicable geographic locations based on source of real-time data.
- Enhanced or advanced wait treatment such as self-service or predictive offers to callers.

Related links

Feature description on page 22

Call classification

Experience Portal provides the facility to detect and classify a call. It detects what is on the other end of the call; human, fax, or answering machine.

Following are the detection types:

- Tone Based
  - Busy Signal, Fax Machine
  - More Accurate Detection
- Speech based
  - Live Voice, Answering Machine
  - Less Accurate - A person who answers with a long welcome might be interpreted as an answering machine
  - Application must be flexible for Live Voice, Answering Machine, or timeout

Related links

Feature description on page 22

Zoning

Zoning is the capability of partitioning a system into multiple zones. Zoning provides the following advantages to customers who are located at geographically distributed sites and to customers with a large system at a single location by:

- Easy management of large systems, such as MPPs.
- Effective management of WAN traffic.
- Local access and transport area considerations for outbound calls.

Related links

Feature description on page 22
Zone architecture on page 30
Resource management and licensing on page 31
Moving resources between zones on page 32

Zone architecture

Zones are extended systems of Experience Portal. A zone acts as a central location for all resource management and configuration. Each zone is either coresident to create artificial boundaries for resource management, or is deployed remotely so that all RTP traffic is contained within the location represented by the zone. The entire data traffic of primary EPM crosses zonal boundaries and includes configuration information, control, status information, and report data. SIP traffic can also cross zonal boundaries.

The zone specific resources are:

- Auxiliary EPMs
- Media servers
- Speech servers (ASR and TTS)
- VoIP configurations
- Email connections
- SMPP and HTTP connections
- Applications
- HTML redirector

Note:

Each zone must have a configured proxy. The proxies are shared across zones and provides call distribution across zones.

The system stores the resources in the primary EPM configuration database. The primary EPM OMS Poller distributes zone-specific data to each zone. The primary EPM performs the following functions:

- Downloads zone-specific configuration to Media servers, for example:
  - ASR/TTS resources assigned to a zone
  - Proxy configuration assigned to a zone
  - H.323 configuration assigned to a zone
  - Applications assigned to a zone

    Note:

    Application servers are not configured and, therefore, are not assigned to a zone. Such Application servers are common resources.
- Polls for status and statistical data from each server.
- Manages the operational states, for example, **Starts**, **Stops**, **Restarts**, **Reboots**, and **Halts**.
- Downloads the report data, for example, the Contact Summary and Contact Detail reports.

Related links

Zoning on page 30

Resource management and licensing

The following are the three levels of resource management in Experience Portal :

1. Zones
2. Organizations within a zone
3. Applications within an organization that is in the zone

The administrator manually assigns the licenses to each zone using Allocations. Zones do not share licenses between each other. If a zone is short of licenses, the system does not automatically allocate extra licenses to that zone from other zones containing unused licenses. The administrator must control the resource allocation to zones effectively, so that each zone gets the required number of licenses.

Related links

Zoning on page 30

Moving resources between zones

Resources assigned to a zone can be moved from one zone to another zone. However, there are certain restrictions for moving a resource from one zone to another.

Resource	Restrictions
Applications	No applications can be moved from one zone to another.
Organizations	No applications are configured in the zone from which the resource is being moved.
Auxiliary EPM servers	If a co-resident SMS processor uses an SMPP connection which is not shared, changing zones is not possible.
Media servers	The media server being moved must be stopped.
ASR servers	All media servers are stopped in the zone from which the resource is being moved.
TTS servers	
H.323 connections	
SIP connections	
SMPP connections	All auxiliary EPM servers must be stopped in the zone from which the resource is being moved.
HTTP connections	
Email connections	

Related links

Zoning on page 30

Chapter 3: Interoperability

Product compatibility

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

Operating system compatibility

The following Linux versions are supported for fresh installations of Experience Portal 8.x and upgrades of Experience Portal from 7.x to Experience Portal 8.x:

- RHEL 7.x 64 bit and RHEL 8.x 64 bit or later
- Avaya Linux based on RHEL 8.x or later

For upgrades from Experience Portal 7.x to Experience Portal 8.1, the operating system upgrade is mandatory. The following Linux versions are supported for Experience Portal 8.1:

- Red Hat Enterprise Linux Release 7.x 64 bit and 8.x 64 bit or later
- Avaya Enterprise Linux RH8.2.64-AV12EP8 or later

Note:

For security fixes, you must upgrade the operating system to RHEL 7.x 64 bit or RHEL 8.x 64 bit or Avaya Linux.

The Avaya-provided ASP 110 server offer includes Enterprise Linux Installer, which installs the Avaya provided RHEL operating system.

The Avaya-provided ASP 130 server offer includes a VMware ESXi hypervisor. The operating system must be installed as an on-site fresh installation.

Browser compatibility

Experience Portal supports the following web browsers:

- Internet Explorer 11
- Mozilla Firefox 44

Orchestration Designer requirements

Experience Portal supports the applications that are developed using Avaya Orchestration Designer 6.0 and later.

For detailed Orchestration Designer requirements, see the Orchestration Designer documentation on the Avaya Support website at https://support.avaya.com.

Proactive Outreach Manager compatibility

Experience Portal supports Proactive Outreach Manager (POM).

Intelligent Customer Routing compatibility

Experience Portal supports Intelligent Customer Routing (ICR).

Third-party product requirements

The Experience Portal network includes the following external system servers:

- Speech servers
- Email servers
- SMS servers
- Application servers

External database requirements

The performance of the Experience Portal internal database degrades when 5 to 10 million records exist in any table. When you expect the number of calls or number of application-generated report records to exceed these values, you must use an external database.

The external database can be a new or existing database created in:

- Microsoft SQL Server 2010 and greater
- MySQL 5.6 and greater
- MariaDB 10.5 and greater
- Oracle 11g and greater
- PostgresSQL 9.6.x and greater

Note:

Avaya has tested Experience Portal with Oracle and SQLServer reporting databases containing approximately 50 million total records without any issues. Due to variances in database hardware and network performance, Avaya cannot provide a finite maximum number of records before the database reaches its practical limit. Scheduled reports are not subject to timeouts and can be used when on-demand report generation begins to time out. However, record insertions must be completed within 60 seconds to avoid web service time-outs and perpetual retries. Increasing the web service time-outs is not recommended. When insert time-outs occur regularly, Avaya recommends that you lower the record retention periods in the Report Data Configuration page. Fewer records mean faster insertions and faster report generation.

Important:

The administration and maintenance of the external reporting database and the periodic maintenance of the indexes is a customer responsibility.

Speech application requirements

The following technologies are required for Experience Portal speech applications:

	Description
CCXML	Experience Portal supports Call Control eXtensible Markup Language (CCXML) applications that comply with most of the standards defined in Call Control eXtensible Markup Language (CCXML). Of these standards, Experience Portal does *not* support: • The <createccxml> tag. • The <move> tag. • The <join> tag for dialogs. Dialogs can attach to a call or conference using the <dialogprepare> or <dialogstart> tags. • The <unjoin> tag for dialogs. Dialogs remain attached to a call or conference session for the entire duration of the dialog or the session, whichever ends first. • The Basic HTTP Event I/O Processor described in Appendix K of the W3C Working Draft. For more information, see the W3C CCXML Version 1.0 Web site.
VoiceXML	Voice eXtensible Markup Language (VoiceXML) applications are required to comply with the W3C VoiceXML Version 2.1 Recommendation. For more information, see the Voice Extensible Markup Language (VoiceXML) Version 2.1, W3C Recommendation Web site.
ASR	If you plan to use Automatic Speech Recognition (ASR) technology in your speech application, you must adhere to the Automatic Speech Recognition (ASR) requirements. For more information, see the Speech Recognition Grammar Specification Version 1.0, W3C Recommendation Web site.
TTS	If you plan to use Text-to-Speech (TTS) technology in your speech application, you must adhere to the Text-to-Speech (TTS) requirements. For more information, see the Speech Synthesis Markup Language (SSML) Version 1.0, W3C Recommendation Web site.

Note:

Speech applications designed and created with the Orchestration Designer tool meet these requirements and recommendations.

Speech application development tools

Any speech application that is compliant with the VoiceXML Version 2.1 Recommendation or Call Control eXtensible Markup Language (CCXML) will run in an Experience Portal system, regardless of the tool in which the application was created. Avaya recommends that you create your speech applications with Orchestration Designer.

Orchestration Designer is an Eclipse plug-in that provides an integrated GUI for application design and implementation. It creates speech applications that automatically conform to the Experience Portal requirements and recommendations.

In addition, Experience Portal automatically includes all Orchestration Designer applications in the Application Summary report and Application Detail report. If you want these reports to display messages and status information from an application developed in a third-party tool, you must manually log the messages and status information from that application using the Application Logging web service.

Application server requirements

In an Experience Portal network, the application server is a web server that hosts your Voice eXtensible Markup Language (VoiceXML) and VoiceXML speech applications. The application server also hosts textXML and HTML applications that are developed with Orchestration Designer.

Experience Portal provides the capability to load balance or failover between two instances of application servers, provided that you set up third-party products.

Dedicated server requirements

If you are installing the Experience Portal Manager (EPM) and the MPP software on different servers, you must also install the Application server on a different server.

Single server requirements

Two options are available for single server configurations:

- You can use a coresident Tomcat to host the applications.
- You can use a separate Application server that is offboard the EPM and MPP servers.

To install an Application server on the same server as the Experience Portal software, use the following versions of the server:

- Tomcat 9

  Note:

  Avaya Experience Portal includes an installation script for the Tomcat 9 application server. If you select any other version of Tomcat, you must manually install the Application server.

- Java version 17.x, which is automatically installed when you install the Avaya Experience Portal software.
- WebLM 8.x, which is automatically installed when you install the Avaya Experience Portal software.

Additional information

For more information about:

- Java, go to https://www.azul.com/.
- WebSphere Express, go to http://www.ibm.com/software/webservers/appserv/express/.
- Tomcat, go to http://jakarta.apache.org/tomcat/.
- See the Orchestration Designer documentation from http://avaya.com/support.

Application Logging web service

Experience Portal supports Axis 2.0 Application Logging web service.

If you use Axis 1.4, you must migrate the applications to Axis 2.0 before upgrading to Experience Portal 8.1.

Text application requirements

The following technologies and protocols are required for Experience Portal text applications:

	Description
TextXML	Textxml is modified Voicexml to handle text messages and text processing capabilities. Textxml starts with `<Textxml>` tag, and follows the same structure as Voicexml containing forms, vars, blocks and grammars. Experience Portal supports only message applications created in Orchestration Designer, which comply with TextXML. For more information, see the Orchestration Designer help.
SMPP protocol version 3.4 HTTP protocol	SMS Server functions as the Gateway to Short Message Service Center (SMSC). The SMS processor connects to the SMSC with SMPP protocol or HTTP protocol, for sending and receiving short messages.
IMAP	Experience Portal supports Internet Messages Access Protocol (IMAP) over TCP or TLS for inbound emails.
SMTP	Experience Portal supports SMTP over TCP or TLS for sending emails.

Note:

Text applications designed and created with Orchestration Designer meet these requirements and recommendations.

Speech server requirements

If your speech applications require Automatic Speech Recognition (ASR) or Text-to-Speech (TTS) resources, you can purchase and install third-party speech servers. All ASR servers must come from the same vendor, and all TTS servers must come from the same vendor. You can, however, have ASR servers from one vendor and TTS servers from a different vendor.

Note:

See the table below for recommended versions of Nuance and Loquendo speech servers. Check Avaya DevConnect or speech support guide for information on other vendors.

Supported speech server versions for ASR and TTS

Speech Server	Components	Minimum version	Recommended version
Nuance 9	Nuance Speech Server (NSS)	5.1.9	5.1.11
	Recognizer	9.0.19	9.0.21
	Vocalizer	5.0.7	5.0.9
Nuance 10.2	Nuance Speech Server (NSS)	6.2.6	6.2.10
	Recognizer	10.2.4	10.2.8
	Vocalizer	6.0.2	6.0.6
Nuance 10.5	Nuance Speech Suite (includes the following components)	10.5.3	10.5.3
	Nuance Speech Server (NSS)	6.5.2	6.5.2
	Recognizer	10.5.2	10.5.2
	Vocalizer	6.2.3	6.2.3
Nuance 11.0.2	Nuance Automation Assist	4.0.1	4.0.1
	Nuance License Manager	11.14.3	11.14.3
	Nuance Management Station	6.0.1	6.0.1
	Nuance Recognizer	11.0.1	11.0.1
	Nuance Speech Product Documentation	11.0.1	11.0.1
	Nuance Speech Server	7.0.2	7.0.2
	Nuance Vocalizer for Enterprise	7.1.6	7.1.6
	Nuance Dragon Voice (includes the following components)		
	Krypton recognition engine	3.2.0	3.2.0
	Natural Language Engine (NLE)	3.2.0	3.2.0
	Nuance Meaning Extraction Engine (NMEE)	7.0.3	7.0.3
	Natural Language Processing (NLP) service	1.0.2	1.0.2
	Nuance Resource Manager	1.0.1	1.0.1
	Nuance Text Processing Engine (NTpE)	3.2.0	3.2.0
Nuance 11.0.9	Nuance License Manager	11.16.5	11.16.5

Table continues…

Speech Server	Components	Minimum version	Recommended version
	Nuance Recognizer	11.5.0	11.5.0
	Nuance Speech Server	7.6.0	7.6.0
	Nuance Vocalizer for Enterprise	21.06.0	21.06.0
Loquendo LSS	Loquendo Speech Suite (LSS)	See recommended version	Windows: LSS 7.0.18 + patch 3 Linux: LSS 7.0.10 + patch 3
	ASR	See recommended version	LASR 7.9.1 + patch 15
	TTS	See recommended version	LTTS 7.23.0
Loquendo LMS	Loquendo MRCP Server (LMS)	See recommended version	Windows: LMS 7.2.1 + patch 3 Linux: LMS 7.2.2 + patch 2
	ASR	See recommended version	LASR 7.10.1 + patch 3
	TTS	See recommended version	LTTS 7.25.2 + patch 1

Important:

Support for Loquendo speech servers is limited to a maximum of 100 ports of ASR and 100 ports of TTS per Experience Portal system.

MRCP support

Speech Server	MRCP v1 Support	MRCP v2 Support
Nuance	Yes	Yes
Loquendo	Yes	No

SRGS support

Speech server	SRGS support	SRGS format support with SISR tag
Nuance	Yes	Yes
Loquendo	Yes	Yes

NLSML and EMMA Recognition Result support

Speech server	NLSML Recognition Result support	EMMA Recognition Result support
Nuance	Yes	Yes
Loquendo	Yes	Partially supported

Additional information

For more information about Nuance and Loquendo servers, see http://www.nuance.com.

SIP requirements

For SIP connections, Experience Portal requires Avaya Aura® Session Manager with Communication Manager or a third-party SIP Gateway or SIP Trunk. For the latest and most accurate compatibility information, go to http://support.avaya.com/CompatibilityMatrix/Index.aspx.

H.323 requirements

For H.323 connections, you must have Communication Manager version 7.0 or later.

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

You must use Communication Manager with the Avaya Special Application SA8874 feature. This combination provides:

- VoiceXML supervised transfers. Without the SA8874 feature, supervised transfers have no access to call progress information and behave like a blind transfer.
- The Application Interface web service for outbound calling. Without the SA8874 feature, the web service has no access to call progress information and may start a VoiceXML application even when the connection attempt receives a busy signal.

Note:

The SA8874 feature is prerequisite to support call classification in an H.323 environment for Experience Portal and Proactive Outreach Manager with Communication Manager. Communication Manager provides the SA8874 Green Feature. However, you must turn the feature on for implementation.

Feature Comparison between H.323 and SIP

This table compares SIP, standard H.323, and H.323 with the Avaya Special Application SA8874 feature enabled in Communication Manager.

Feature	H.323	H.323 with SA8874 feature	SIP
Outbound calling using the Application Interface web service	Partially supported. No call progress information is available, so an application may start before a call is answered.	Supported	Supported
Call conferencing	Supported	Supported	Supported
Call classification	Supported	Supported	Supported
Blind transfer	Supported	Supported	Supported
Supervised transfer (also called consultative transfer) If a connection cannot be established, use the Consultative Transfer feature in Experience Portal to allow the application to regain control of the call.	Operates like a blind transfer. The only supported VoiceXML event for this transfer is error.connection.noroute.	Supported	Supported
Bridge transfer See also Bridge transfers in a mixed SIP or H.323 environment on page 42	Partially supported. No call status information, such as "line is busy", is available.	Supported	Supported except for the VoiceXML `<transfer>` tag's `connecttimeout` parameter, which is not supported
DTMF detection Experience Portal supports only out-band DTMF detection.	Supported	Supported	Supported In case of SIP VoIP connection, the signaling group doesn't support the out- band option. It supports the in-band and RTP-payload DTMF options.
Playing prompt files	Supported	Supported	Supported
Recording	Supported	Supported	Supported
Converse-on vectoring	Supported	Supported	Not supported
Encryption options	• Disabled • Advanced Encryption Standard (AES) • Avaya™ Encryption Algorithm (AEA)	• Disabled • AES • AEA	• Disabled • TLS • SRTP
Quality of Service	Supported	Supported	Supported

Table continues…

Feature	H.323	H.323 with SA8874 feature	SIP
User to User Information (UUI)	Not supported	Not supported	For an incoming call, UUI values are populated in the VoiceXML session variables for both UUI and Application to Application Information (AAI).
Universal Call Identifier (UCID)	Supports the capability to receive UCID over H323 from Communication Manager. This capability is available in Communication Manager 5.2. To enable this feature, you need to administer ucid-info on button 10 on the 7434ND stations used by Experience Portal. For more information, see *Administering Avaya Experience Portal*.		Supports the capability to both send and receive UCID. For more information, see *Administering Avaya Experience Portal*. **Note:** Also supports the GSLID used by AACC
Switch failover	An alternate gatekeeper address can be specified in the EPM. Communication Manager can supply an alternate gatekeeper address list.		Experience Portal does not supply additional support, but the Avaya Aura® Session Manager hardware has failover support and MPPs can be configured as members of an adjunct in ASM.
Merge (Refer with replaces)	Not supported	Not supported	Supported

Bridge transfers in a mixed SIP or H.323 environment

If you have both SIP and H.323 connections defined in your Experience Portal system, Experience Portal handles bridge transfers in the following manner. For an outbound call with:

- `SIP` or `SIPS` in the `ToURI` field, a SIP outbound channel must be available.
- `TEL` in the `ToURI` field, Experience Portal tries to get an outbound port from the same H.323 port group. If none are available, Experience Portal tries any H.323 port.

  If no H.323 ports are available, Experience Portal converts `TEL` into `SIP` in the `ToURI` field and tries to get a SIP outbound channel.

Minimum server machine hardware requirements

Customer supplied servers must meet the following minimum specifications to run Avaya Experience Portal:

- Compatibility with a supported version of Red Hat Enterprise Linux Server

  For information about hardware compatibility, go to the *Certified Hardware* section of the Red Hat website, http://www.redhat.com.

- Dual Quad Core 1.6 GHz Pentium 4 or equivalent processors
- 4 GB of RAM
- 120 GB Disk, 7200 RPM
- One 100/1000 Base-T Ethernet controller that is full duplex (onboard Network Interface Cards (NICs)
- DVD drive
- Keyboard
- Monitor
- Mouse
- Avaya Secure Access Link (SAL) or Avaya EASG solution

  If you purchase a maintenance agreement with Avaya Services, the Experience Portal system requires SAL or Avaya EASG solution so that Avaya Services can remotely access the system for maintenance purposes. Contact Avaya Support to determine the version of SAL and Avaya EASG supported.

PBX requirements

The PBX must be accessible to the Experience Portal servers through a LAN, and the PBX must run the appropriate version of Communication Manager. The required Communication Manager version is based on whether you want to use H.323 connections, SIP connections, or both.

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

Connection type	Version required
H.323 connections	Communication Manager version 7.0 or later
H.323 with supervised transfer or the Application Interface web service for outbound calls	Communication Manager 7.0 with the Avaya Special Application SA8874 feature
SIP	Avaya Aura® Session Manager version 7.0 or later with either Communication Manager version 7.0, a third-party SIP Gateway, or SIP Trunk
SIP with SRTP	Avaya Aura® Session Manager version 7.0 or later with Communication Manager version 7.0

Important:

You are responsible for managing and maintaining the PBX.

LAN requirements

Connectivity requirements

Experience Portal requires a 100/1000 Base-T LAN full duplex network switch connection so that Experience Portal servers can communicate with each other, with any other speech servers, any application servers, and any Private Branch Exchange (PBX) servers.

Each server in your Experience Portal system must be able to connect to all the other servers in the system using the host names of the other servers. You must use a Domain Name Server (DNS) for this purpose.

Server name requirements

Each Experience Portal server must have a static IP address and a host name. Each host name must be unique and cannot contain a `.` (period) or a (space) character.

Site requirements

Verify that the site where you are installing the Experience Portal hardware platform is equipped with the following:

- Rack space for the servers that host Experience Portal.
- At least one network connection for each Experience Portal server. Depending on your network topology, two network connections might be required for each media server.
- Power supply.
- (Optional) Analog telephone line provisioned for Avaya Secure Access Link (SAL) or the Avaya Access Security Gateway (ASG) solution.

Chapter 4: Performance specifications

Capacity and scalability specification

Single zone system capacities

Experience Portal resource	Capacity
System limits	
Media servers	30 servers
Telephony ports	10,000 ports
SIP	10,000 ports
H.323	5,000 ports

Multi-zone system capacities

Experience Portal resource	Capacity
System limits	
Zones	15 zones
Media servers	70 servers
Telephony ports	50,000 ports
SIP	50,000 ports
H.323	10,000 ports
Per zone limits	
Media servers	30 servers
Telephony ports	10,000 ports
SIP	10,000 ports
H.323	5,000 ports

Media server capacities

Experience Portal resource	Capacity[1]
Calls (Standalone media server)	1500 simultaneous calls.
Inbound calls	1500 simultaneous calls.

Table continues…

[1] Varies based on application complexity, audio codecs, server hardware, and other factors.

Experience Portal resource	Capacity[1]
Outbound calls	1500 simultaneous calls.
Calls (Single-Box system)	1500 simultaneous calls.
Inbound calls	1500 simultaneous calls.
Outbound calls	1500 simultaneous calls.

Multi-media server capacities

Experience Portal resource	Primary EPM capacity (messages/hour)	Auxiliary EPM capacity (messages/hour)	Single-box system capacity (messages/hour)
Email Messages[2][3]			
Outbound only	25,000	50,000	5,000
Inbound only	12,500	25,000	2,500
Bi-directional	8,000 Inbound 8,000 Outbound	16,000 Inbound 16,000 Outbound	1600 Inbound 1600 Outbound
SMS Messages[2]			
Outbound only	25,000	50,000	5,000
Inbound only	12,500	25,000	2,500
Bi-directional	8,000 Inbound 8,000 Outbound	16,000 Inbound 16,000 Outbound	1600 Inbound 1600 Outbound

Note:

Check with your SMS provider for any capacity limitations for inbound or outbound SMS messages. Carrier regulations often require more restrictive capacity limitations when using long codes.

HTML Application capacities

Experience Portal Resource	Primary EPM Capacity (launches/hour)	Auxiliary EPM Capacity (launches/hour)	Single-box System Capacity (launches/hour)
Inbound only	12,500	25,000	2,500

Profile size specification

The following are the recommended minimum profile specifications for Avaya Experience Portal 8.1:

[1] Varies based on application complexity, audio codecs, server hardware, and other factors.
[2] Varies based on application complexity, server hardware, service provider, and other factors.
[3] Large email attachments substantially reduce expected throughput.

MPP Profiles	MPP Port Capacity	Standalone MPP	Standalone EPM	Single server	ASP 110/130 Server Support		
					Profile 3 (110)	**Profile 4 (110, 130)**	**Profile 5 (110, 130)**
Entry	250	4 vCPU + 4GB RAM*	2 vCPU + 4GB RAM	4 vCPU + 4GB RAM	40 vCPU + 48GB RAM Dual 10 core	28 vCPU + 96GB RAM Single 14 core	56 vCPU + 192GB RAM Dual 14 core
Small	500	8 vCPU + 8GB RAM*	6 vCPU + 12GB RAM*	8 vCPU + 8GB RAM			
Medium (Typical)	1000	8 vCPU + 16GB RAM*		8 vCPU + 16GB RAM			
Large	1500	12 vCPU + 24GB RAM*		12 vCPU + 24GB RAM			

** Identifies MPP (x4) and EPM (x1) OVA profile options*

MPP Profiles	MPP Port Capacity	AWS Minimum Profile		GCP Minimum Profile		Azure Minimum Profile	
		MPP	**EPM**	**MPP**	**EPM**	**MPP**	**EPM**
Entry	250	t2.xlarge 4 vCPU + 16GB RAM	c5.large 2 vCPU + 4GB RAM	e2-standard-4 4 vCPU + 16GB RAM	e2-medium 2 vCPU + 4GB RAM	F4s_v2 4 vCPU + 8GB RAM	F2s_v2 2 vCPU + 4GB RAM
Small	500	c5.2xlarge 8 vCPU + 16GB RAM	c5.2xlarge 8 vCPU + 16GB RAM	e2-standard-8 8 vCPU + 32GB RAM	e2-standard-8 8 vCPU + 32GB RAM	F8s_v2 8 vCPU + 16 GB RAM	F8s_v2 8 vCPU + 16GB RAM
Medium (Typical)	1000						
Large	1500			e2-standard-16 4 vCPU + 64GB RAM		F16s_v2 12 vCPU + 32GB RAM	

Important:

Profile size recommendations are based on performance test results obtained from testing with G.711 and G.729 codecs. Note the following considerations:

- Call scenarios are based on simple call flows. Increasingly complex call flows may require an increase to resource allocation.
- Cloud platform recommended profiles are the closest match to On-Premise validated profiles.
- VMware Host server has Intel(R) Xeon(R) Gold 6230 CPU @ 2.10GHz CPUs that may deliver improved performance over other CPUs. Lower benchmarked CPUs may require an increase to resource allocation.

Traffic specification

Network topology

Partitioning your Experience Portal network increases the available network bandwidth.

- Experience Portal physical server Avaya Common Server includes four Gigabit network interface cards (NICs) per server.
- Smaller Experience Portal deployments might not require network partitioning to achieve a reliable system.
- Although your Experience Portal system might function without network partitioning, as a minimum Experience Portal requirement, each server must be equipped with two NICs.
- Corporate Network

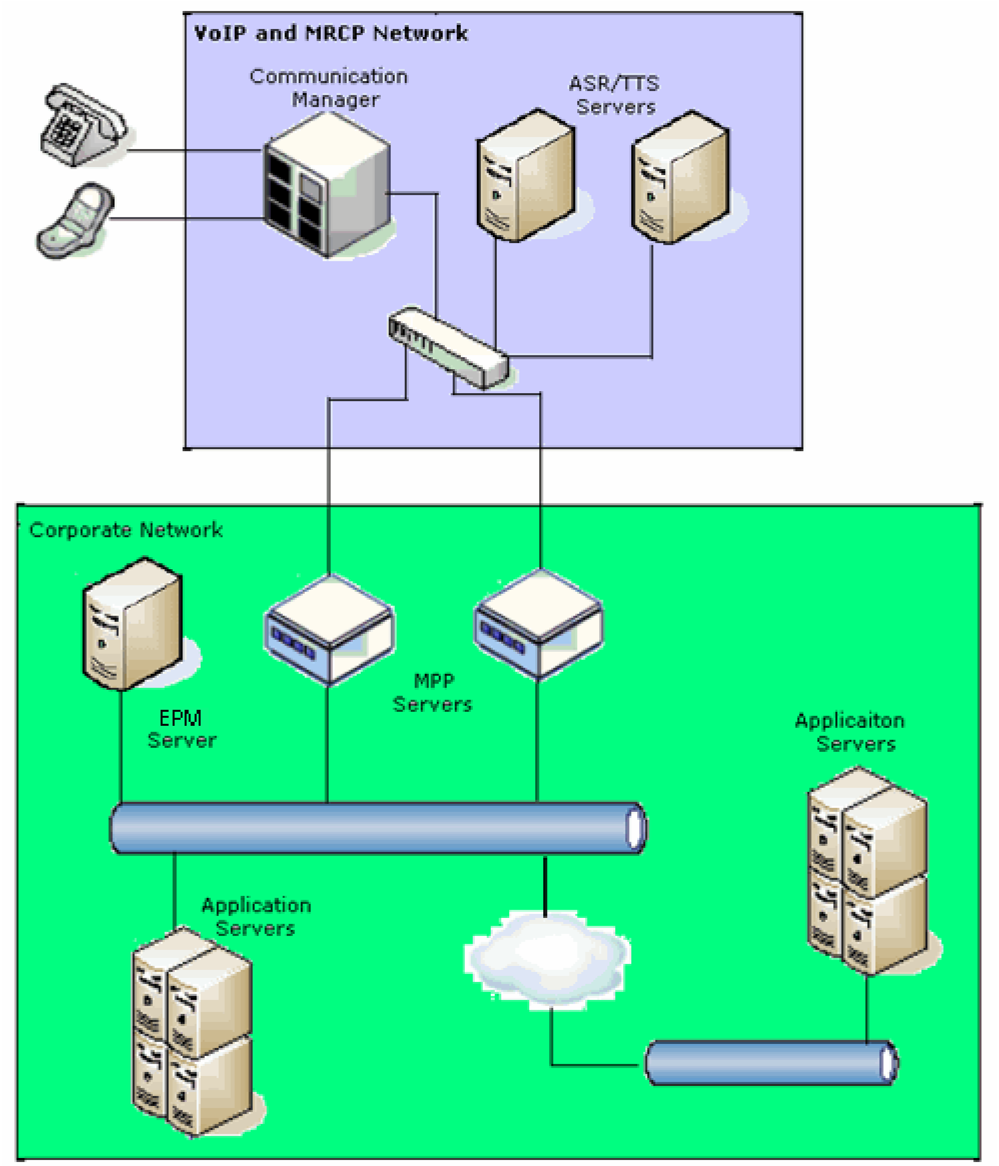
  The corporate network segment carries the network traffic for Media Processing Platform (MPP) system configurations and MPP monitoring. The Experience Portal Manager (EPM) downloads the system configurations to the MPPs and also monitors the MPPs. This segment also carries the network traffic generated by VoiceXML application execution.
- VoIP network

  The VoIP network segment carries the network traffic between the Communication Manager and the MPPs for VoIP telephony processing.
- Media Resource Control Protocol (MRCP) network

  The MRCP network transports the network traffic between the MPPs and ASR/TTS servers for text rendering and speech processing.

Network topology with two network segments

The following network topology figure shows an Avaya Experience Portal network configuration consisting of two network segments:



In this example, the network configuration is segmented into two networks:

- Corporate network

  The corporate network segment carries the network traffic for MPP system configurations and MPP monitoring. The EPM downloads the system configurations to the MPPs and also monitors the MPPs. This segment also carries the network traffic generated by VoiceXML application execution.

- VoIP and MRCP network

  The VoIP and MRCP network carries the network traffic between the Communication Manager and the MPPs and the traffic between the MPPs and ASR/TTS servers.

Failover best practices

Failover overview

When designing an Experience Portal system, you must take into consideration the results of equipment failure. In addition to the failure of an Experience Portal server (that is Primary EPM, Auxiliary EPM, or MPP), you must also consider the failure of servers that Experience Portal depends on. For example, application servers, speech servers, and telephony servers. Typically, Experience Portal systems are designed to withstand the failure of any single server wherein, you must have enough servers of each type so that the system can continue to process calls and messages at full capacity even if one server goes out of service. Such systems are said to be highly available. Some customers might implement a second complete system at a different location. The purpose of the second system is to handle cases where some large-scale problem such as fire, flood, or power outage takes all the servers in the original system out of service at the same time. This method is known as disaster recovery.

High availability

Experience Portal provides the option to create highly available systems. You must have the required number of servers.

This section explains various high availability instances in the Experience Portal system.

Note:

Each topic in this section depends on the applications you use in your environment and might be applicable to your system.

Applications

For high availability support in applications, you must install each application on two different application servers.

When you configure the application in the EPM web interface, configure two URLs for the application.

If Experience Portal cannot load the application from one URL, Experience Portal automatically loads the application from the second URL.

Speech servers

For high availability support in speech server, you must install the automatic speech recognition (ASR) language and the text to speech (TTS) voice on two different speech servers. When you do so, the Experience Portal system automatically sends speech request to the second server if the connection to the first speech server fails.

Note:

Media Processing Platform (MPP) server can only use speech servers with the same zone as the MPP server. If the Experience Portal system includes multiple zones, then each zone must contain at least two speech servers. When you do so, the zone continues to operate normally even if the connection to one speech server in the zone fails.

Telephony servers

For high availability support in telephony server, you must have at least two telephony servers.

H.323

If you are using H.323, use the **Change H.323 Connection** page of the EPM web interface to configure two addresses for the Communication Manager gatekeeper. When you do so, Experience Portal automatically connects to second gatekeeper if the connection to the first gatekeeper fails.

SIP

If you are using Session Initiation Protocol (SIP), use the **Change SIP Connection** page of the EPM web interface to configure addresses for multiple SIP proxies. When you do so, Experience Portal automatically connects to the second SIP proxy, Experience Portal if the connection to the first SIP proxy fails.

Inbound calls

An MPP server processes inbound calls.

If the connection to the MPP server fails, the primary EPM shares all telephony ports to the other MPP servers. With this method, the system continues to process calls at full capacity.

Note:

The primary EPM shares only specified number of telephony ports with the MPP server. You can define the telephony ports in the **Maximum Simultaneous Calls** field on the **Change MPP Server** page of the EPM web interface. You must design the system so that even if one MPP server is down, the remaining servers have enough capacity to handle all telephony ports that have been configured.

The MPP server can use only those telephony ports which are in the same zone as the other MPP server. If the Experience Portal system includes multiple zones, then you must ensure that each zone contains at least two MPP servers. When you do so, the system in the zone uses the second server if the connection to the first MPP server fails.

Outbound calls

The Application Interface Web service initiates outbound calls.

There is one instance of the Application Interface web service on the Primary EPM server and another instance on each Auxiliary EPM server. To be highly available, any system that makes outcalls must include at least one Auxiliary EPM server. Client applications invoke the Application Interface web service through a request that includes a URL. That URL includes the host name or IP address of the Primary EPM or the Auxiliary EPM server that hosts the Application Interface web service.

For high availability, client applications must support the following capabilities:

- Detect a failure to process the Application Interface web service on one server and automatically process a different instance of the Application Interface web service on another server.
- The customers client application which sends requests to the Application Interface web service must have knowledge of all EPM's, Primary and Auxiliary, in the customers system and must send the request to a different EPM if the request cannot be completed by an EPM.
- If the Primary or Auxiliary EPM is in the process of being upgraded, then the requests should be directed to the other EPM's in the system.

Inbound email messages

At any given time, only one email processor processes incoming email messages on a particular email connection. That email processor can be on either the Primary EPM or an Auxiliary EPM server. If an Auxiliary EPM server goes out of service while processing an email connection, the Primary EPM automatically assigns that email connection to another email processor.

If an email connection is assigned to the email processor on the Primary EPM server at the time that the server goes down, then that email connection remains in the out-of-service mode until the primary EPM server restores the connection. The email connection continues to remain in the out-of-service mode because of network failure in the primary EPM server. In addition, you cannot change the Experience Portal configuration as you cannot again access to the EPM web page. Therefore, you must configure email processors on two Auxiliary EPM servers rather than configuring the email processor on the Primary EPM server along with an email processor on an Auxiliary server.

An email processor can service only those email connections that are associated with the same zone as the email processor. If your Experience Portal system includes multiple zones, then each zone that contains an email connection must contain at least two email processors. When you do so, the system processes email messages through the second email processor if the connection to the first email processor fails.

Outbound email messages

For sending outbound email messages, each email connection is shared among all available email processors. You must configure atleast two email processors so that messages are sent even if one of the processors is out of service.

The email processor uses the service email connection in the same zone as the email processor. If the Experience Portal system includes multiple zones, then each zone that contains an email connection must contain at least two email processors. When you do so, the system processes email messages even if one email processor in that zone malfunctions..

Inbound SMS messages

Inbound SMS messages can only be received via an SMPP connection. If you configure an SMPP connection to be shared, the system shares the connection with all available SMS processors. When you do so, when one SMS processor goes out of service, the other SMS processors will automatically continue to process inbound messages.

Note:

Service providers do not support sharing an SMPP connection. In such cases, you must manually assign the connection to a particular SMS processor. If the connection to the SMS processor fails, then the system stops processing messages on the SMPP connection. You must manually assign the SMPP connection to another SMS processor.

If an SMS connection is assigned to the SMS processor on the Primary EPM server at the time the server goes down, then that SMS connection will remain out of service until the Primary EPM server comes back up. The SMS connection remains in the out-of-service mode because of the network failure in the primary EPM. In addition, you cannot change the Experience Portal configuration as you cannot gain access the EPM webpage. Therefore, you must configure SMS processors on two Auxiliary EPM servers rather than configuring the SMS processor on the Primary EPM server along with an SMS processor on an Auxiliary EPM server.

An SMS processor can only service SMS connections that are associated with the same zone as the SMS processor. If your Experience Portal system includes multiple zones, then each zone that contains an SMS connection should contain at least two SMS processors so SMS messages in that zone can be processed even if one SMS processor in that zone goes down.

Outbound SMS messages

Outbound SMS messages can be sent over either an SMPP connection or an HTTP connection. Service providers might not share an SMPP connection with SMS processors. However, service providers can share HTTP connections with SMS processors.

For sending outbound SMS messages, each HTTP connection and each sharable SMPP connection is shared among all available SMS processors. You must configure atleast two SMS processors configured. When you do so, the system establishes the connection with the secondary SMS processors if the connection to the primary SMS processor fails.

If an SMPP connection cannot be shared, you must manually assign the connection to a particular SMS processor. If the connection to the SMS processor fails, the system stops processing messages on the SMPP connection. You must manually assign the SMPP connection to another SMS processor.

During a network failure if the system shares an SMS connection to the SMS processor, then the SMS connection remains in the out-of-service mode until the primary EPM server restores the connection. The SMS connection remains in the out-of-service mode because of the network failure in the primary EPM. In addition, you cannot change the Experience Portal configuration as you cannot gain access the EPM webpage. Therefore, you must configure SMS processors on two Auxiliary EPM servers rather than configuring the SMS processor on the Primary EPM server along with an SMS processor on an Auxiliary EPM server.

An SMS processor can service only those SMS connections that are associated with the same zone as the SMS processor. If the Experience Portal system includes multiple zones, then you must ensure that each zone contains at least two SMS processors. When you do so, the system processes the SMS messages even if one SMS processor in that zone goes down.

Inbound HTML launch requests

Inbound HTML launch requests can be received only through the application interface web service.

The HTTP request from a mobile browser is received by the Redirector application. The Redirector processes the request and makes an application interface web service request to Experience Portal to launch the appropriate Orchestration Designer HTML application. After the Orchestration Designer HTML application is launched, the Redirector application sends a redirect request to the mobile browser. From that point, the mobile browser communicates directly with the Orchestration Designer HTML application.

The Redirector application serves the following purposes:

- To provide load balancing and failover for launching HTML applications.
- To hide sensitive data that gets passed from Experience Portal to the Orchestration Designer runtime.
- To prevent HTML applications from being launched with outdated configuration parameters.

Enforcement of HTML launch requests is systemwide and handled by all the EPM servers configured on the system. If an EPM server goes down, then the HTML launch request can be handled by another EPM server without any loss of capacity.

If your Experience Portal system includes multiple zones, then you must configure a redirector in each zone that is expected to launch HTML applications because the redirector is not zone aware. The application interface web service only processes requests for applications configured in the same zone as the server on which the web service is running.

Application logging

There is one instance of the Application Logging web service on the Primary EPM server and another instance on each Auxiliary EPM server. To be highly available, any system that uses the Application Logging web service must include at least one Auxiliary EPM server. Also, these systems should use an external database that is highly available. This is because requests to the Application Logging web service running on an Auxiliary EPM server will fail when the Primary EPM server is down, unless the system is configured to store report data in an external database.

Client applications invoke the Application Logging web service through a request that includes an URL. The URL includes the host name or the IP address of the Auxiliary or the Primary EPM server that hosts the Application Logging web service.

For support in the HA mode, client applications must perform the following:

1. Detect a failure to process the Application Logging web service on the primary server.
2. Use the other instance of the Application Interface web service from the secondary server.

Note:

You can log in to the application through Orchestration Designer, which uses the Application Logging web service. The Orchestration Designer runtime automatically routes the Application

Logging web service requests to an Auxiliary EPM server if the connection to the primary EPM server fails. The Orchestration Designer runtime caches the log data on the application server to prevent loss of data if:

- all instances of the Application Logging web service are temporarily unavailable.
- the system fails to save the data in the database.

Some applications log the data using the tag <log> that is available in both VoiceXML and CCXML. You can store this data locally on the MPP server that is processing the application. The primary EPM server collects the data periodically with other report data that MPP generates. The data logged using the tag <log> does not go through the Application Logging web service.

Configurable application variables

You can configure application variables using the EPM web interface on the Primary EPM server. Therefore, you cannot change values of configurable application variables during network failure to the Primary EPM server.

The Orchestration Designer runtime reads the configurable application variables through the Application Variables web service. One instance of the Application Variables web service on the Primary EPM server and another instance is on each Auxiliary EPM server.

To be highly available, any system that uses configurable application variables must include at least one Auxiliary EPM server. The Orchestration Designer runtime automatically routes Application Variables web service requests to an Auxiliary EPM server if the connection to the Primary EPM server fails.

The system replicates the values of all configurable application variables from the Primary EPM server to each Auxiliary EPM server. With this process, the Orchestration Designer runtime gets the variable values from an Auxiliary EPM server even when the Primary EPM server is out of service.

Primary EPM functions

If the connection to the Primary EPM server fails, the Auxiliary EPM and MPP servers continue to operate using the previous configuration from the Primary EPM. The system continues to process both inbound and outbound operations for telephone calls, emails, and SMS messages. Since an Auxiliary EPM server has limited capabilities of the Primary EPM server, the system might lose some functionality.

If the connection to the Primary EPM server fails, the system:

- Loses access to the administrative webpages.
- Loses the log or the alarm data that the MPP and the auxiliary EPM servers generate.
- Stops automatic redistribution of telephone ports as MPP servers go in and out of service.
- Stops automatic redistribution of email connections as email processors go in and out of service.
- Stops automatic collection of report data.

- Stops generating SMPP notifications.
- Stops processing email messages on connections assigned to the Primary EPM server.
- Stops processing SMS messages on connections assigned to the Primary EPM server.

Since an Experience Portal system can only contain a single Primary EPM server, you must use a feature of VMware vSphere called High Availability (HA) to provide redundancy. With the HA feature, during network outage in the vSphere server, the system automatically starts all virtual server running on another vSphere server. The affected virtual servers might experience a temporary service interruption when restarting the virtual servers.

For information about configuring the Experience Portal system to use the VMware HA feature, see *Application Notes – Avaya Experience Portal on VMware vSphere*, available on https://support.avaya.com/.

Disaster recovery

To provide recovery from a disaster that disables an entire Experience Portal system, you must set up a second Experience Portal system. The second Experience Portal system must be capable of running all applications as the primary Experience Portal system. Both the Experience Portal systems must also have the same capacity. You must ensure that the second Experience Portal system located in a different geographic location from the primary system to reduce the possibility of both Experience Portal systems facing network outage at the same time.

If you deploy two Experience Portal systems in the network, you might face challenges of using the systems when both systems are operable in normal circumstances.

Active-Active multi-site configuration

In an active-active configuration when both systems are running, the systems share the load of processing calls and messages. The load on each system does not exceed 50% of the capacity of the system. The advantage of this approach is that if one system goes out of service, the other system takes more load without requiring manual intervention. For an active-active configuration, you must purchase twice the number of Experience Portal licenses capacity as you intend to use at any one time.

Active-Active license management

In an active-active configuration, you must ensure that each system has Experience Portal license to provide 100% of the capacity. Each system uses only the local WebLM server that coresides with the Primary EPM server.

Active-Passive multi-site configuration

In an active-passive configuration, one system handles all calls and messages at any given time while the other system remains in the idle state. With this approach, you must manually move the license capacity from one system to another system when one system goes out of service.

The advantage of this approach is that you do not need to purchase more license capacity than you actually use.

Active-Passive license management

To move license capacity from one system to another, you must use a central Enterprise WebLM server. You must install the Experience Portal license file on the Enterprise WebLM server and then configure Enterprise WebLM to give all licensed capacity to the local WebLM that coresides with one of the Primary EPM servers. If the active Experience Portal system fails, you must change the Enterprise WebLM configuration to give all licensed capacity to the local WebLM for the surviving Experience Portal system.

Important:

Ensure that you deploy the Enterprise WebLM server in a separate geographic location from the Experience Portal system that is normally active. If the Enterprise WebLM server is at the same site as the active Experience Portal system, then any disaster that disables the Experience Portal system disables the Enterprise WebLM server. You cannot move the licensed capacity to the disaster recovery Experience Portal system.

License management

Use Web License Manager (WebLM) to manage the licensing of Experience Portal. WebLM is an integral part of the Experience Portal system that is available on the EPM server, and provides licenses to EPM. WebLM that resides on the EPM server is also referred to as Local WebLM. In most small setups of Experience Portal systems, the license is installed on the Local WebLM. An Enterprise or Master WebLM is used in a system that requires redundancy through a WebLM that is installed on a separate server. Enterprise WebLM allocates licenses to WebLM that resides on EPM. The location of Enterprise WebLM is critical to the facility of moving a license from one site to another in the event of a failure.

Local Experience Portal redundancy

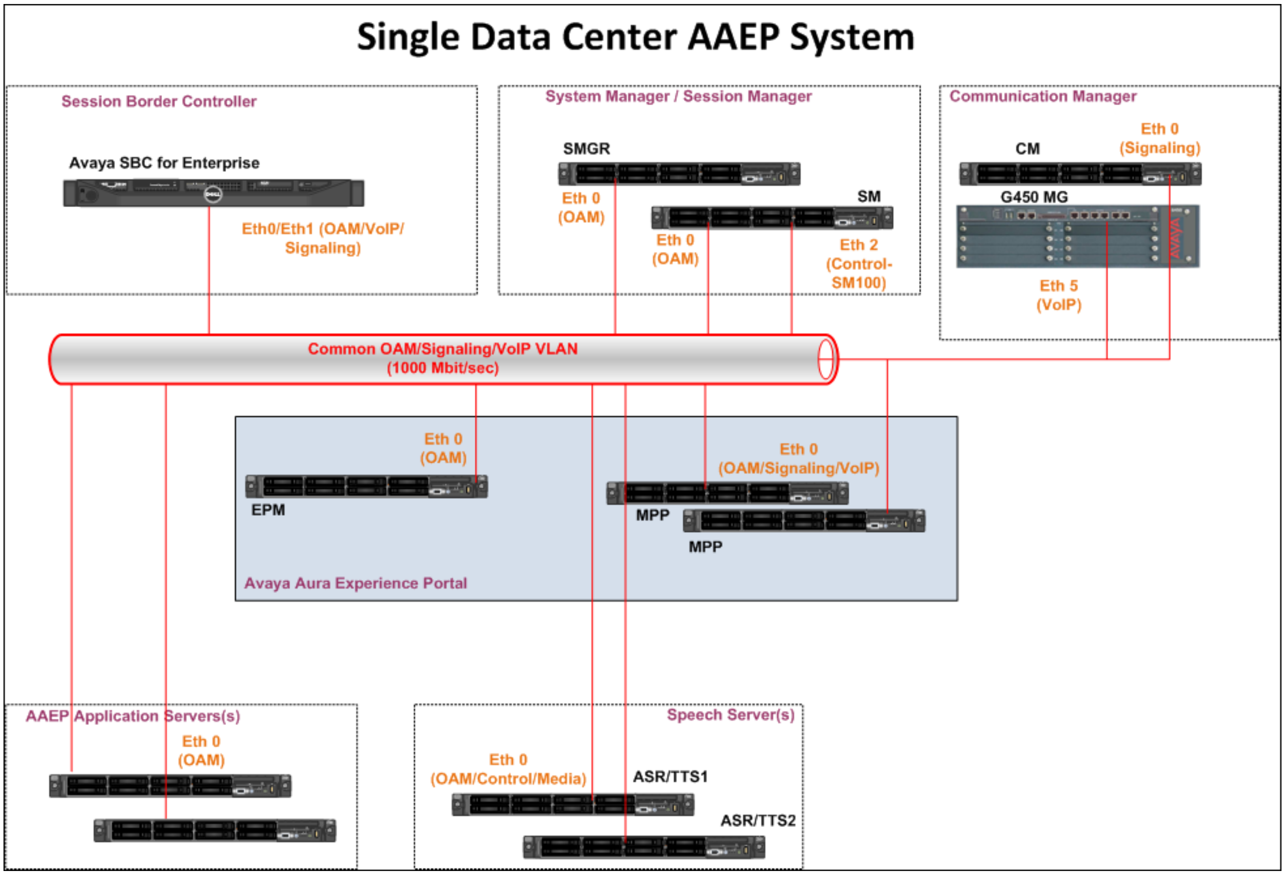
To ensure that the local Experience Portal setup has redundancy for all server components, you must implement additional hardware while configuring Experience Portal. Install a load balancer and additional application servers to provide redundancy for the application server. Ensure that the load balancer is also redundant.

To achieve this redundancy, you must install a highly available solution that utilizes a virtual IP address.

To provide redundancy for the speech servers, install additional speech servers.

The objective is to provide redundancy when a hardware failure occurs.

Experience Portal redundancy does not provide redundancy in the event of a network infrastructure failure.


Single Data Center AAEP System
Session Border Controller
Avaya SBC for Enterprise
Eth0/Eth1 (OAM/VoIP/ Signaling)
System Manager / Session Manager
SMGR
Eth 0 (OAM)
SM
Eth 0 (OAM)
Eth 2 (Control- SM100)
Communication Manager
CM
Eth 0 (Signaling)
G450 MG
Eth 5 (VoIP)
Common OAM/Signaling/VoIP VLAN (1000 Mbit/sec)
Eth 0 (OAM)
EPM
Eth 0 (OAM/Signaling/VoIP)
MPP
MPP
Avaya Aura Experience Portal
AAEP Application Servers(s)
Eth 0 (OAM)
Speech Server(s)
Eth 0 (OAM/Control/Media)
ASR/TTS1
ASR/TTS2

Media Processing Platform

If an MPP fails, Experience Portal Manager detects the failure, reassigns the licenses, and redistributes the ports to other MPPs.

If the failed MPP is assigned to a zone, Experience Portal Manager reassigns the licenses and redistributes the ports to other MPPs within the same zone.

You cannot redistribute ports across zones.

Experience Portal Manager

EPMs are in service at all locations. Even if one location fails, the Master WebLM server distributes all calls to the MPPs at the second location.

System recovery

As with any other application running on a server, it is important to be prepared to do a partial or complete Experience Portal system restoration in case of a disaster.

You must regularly back up Experience Portal systems. Experience Portal includes backup scripts that can be run automatically as a Linux `chron` job and that can perform either full or partial backups on a regular basis.

You must also document the components and settings for the Experience Portal system to facilitate the efforts required to restore the systems. These system records must include the following information:

- Experience Portal customer identification number (CIN), installation location (IL), IP address of the network interface card (NIC), telephone numbers for test calls, and sample account numbers for testing.
- Server names and IP addresses of all Experience Portal system servers, speech servers, database servers, and Application servers.
- A current list of all software, including versions, installed on the system. The software itself should be stored in a safe and easily accessible location.
- Disk partitioning information, so that applications can be restored to the correct locations.
- Information about what needs to be done to restore each application package. All values and parameters that must be entered should be recorded.
- Changes to system defaults.
- Contact information for Avaya as well as for any application vendors, speech vendors, and database vendors that may have provided components used on or with the Experience Portal system.

The Avaya Business Continuity Services can help design and implement disaster recovery plans to support rapid recovery from outages caused by unforeseen circumstances such as natural disasters or other emergency situations. A well-designed disaster recovery plan can help reduce expenses by proactively identifying potentially costly issues related to topology, hardware, software, security, network performance, and business resiliency. For more information about Avaya Business Continuity Services, contact Avaya Support.

Chapter 5: Environmental requirements (hardware only)

Hardware specifications

Avaya Common Server specification HP

Note:

This specification represents the server that Avaya supplies. The specification does not represent the only server that the software runs on.

Base Unit	Quantity	Baseline
Chassis Type	1x	HP 1U DL360G9 8SFF
Processor	2x	2.4 GHz, E5-2620v3, 6 Core
Memory	8x	4GB DDR4 RDIMM
Hard Disk Drives 2.5” SAS	3x	300 GB 10K
RAID Level		5
RAID Controller	1x	P440ar /2G
Serial Port Adapter		Included
Power Supplies	2x	800 WAC
NIC	1x (4 Port)	Quad Port LOM 1GbE
	1x (2 Port)	1Gb 2P 332T Adptr
	2x	PCIe Slot
Optical Drive	1x	DVD - SFF DVD-RW

Avaya Common Server specification DELL

Note:

This specification represents the server that Avaya supplies. The specification does not represent the only server that the software runs on.

Base Unit	Quantity	Baseline
Chassis Type	1x	DELL 1U R630
Processor	2x	2.4 GHz, E5-2620v3, 6 Core

Table continues…

Base Unit	Quantity	Baseline
Memory	8x	4GB DDR4 RDIMM
Hard Disk Drives 2.5” SAS	3x	300 GB 10K
RAID Level		5
RAID Controller	1x	PERC H730 1GB
Serial Port Adapter		Included
Power Supplies	2x	750 WAC
NIC	1x (4 Port)	Broadcom 5720 Dual Port PCIe NIC 1GbE
	1x (2 Port)	Broadcom 5720 Quad Port Card/LOM 1GbE
	2x	PCIe Slot
Optical Drive	1x	DVD-RW SATA

Minimum server hardware requirements for ACP 110 and ACP 130

Avaya Experience Portal supports a new common server ACP 110 (bare-metal) and ACP 130 (VMWare).

Avaya can provide customers a complete bundled solution including hardware. In such cases, the hardware platform for the Avaya supplied servers is ACP 110.

Requirement	Requirement nos.
CPU chipset	S-4114
Server CPU	2
CPU Cores	10
Server Cores	20
Core processing frequency	2.2 Ghz
DRAM	48 Gig
SAS 10K Hard-disks	4
SAS Hard-disk size	600 GB
Virtual Drive	1.8 TB
1 Gig Network ports	6

For more information on ASP 110 and ASP 130 supported profiles, see Profile size specification on page 46.

Environmental specifications

Specification	Value
Operating altitude derating	All temperature ranges are shown at sea level. An altitude derating of 1°C per 300 m (1.8° per 1,000 ft.) to 3048 m (10,000 ft) is applicable.
Storage	Maximum altitude 12,000m (39,370 ft)
Operating	10°C to 35°C (50°F to 95°F). No direct sunlight allowed.
Shipping	-40°C to 65°C (-40°F to 158°F) with a maximum temperature gradation of 20 °C (36 °F) per hour
Maximum wet bulb temperature	28°C (82.4°F)
Relative humidity	Storage maximum humidity of 95% is based on a maximum temperature of 45° C (113°F). Altitude maximum for storage corresponds to a pressure minimum of 70 kPa.
Operating	10% to 80% (non-condensing) with 26 °C (78.8 °F) maximum dew point
Non-operating	5% to 95%

Physical specifications

Specification	HP	Dell
Dimensions	Height: 4.32 cm (1.70 in) Width: 42.62 cm (16.78 in) Depth: 69.53 cm (27.38 in)	Height: 4.28 cm (1.69 in) Width: 48.24 cm (18.99 in) Depth: 70 cm (27.58 in)
Weight	19 kg (42.0 lb) (minimum) 22 kg (48.3 lb) (maximum)	18.6 kg (41.00 lb)

LAN requirements

Connectivity requirements

Experience Portal requires a 100/1000 Base-T LAN full duplex network switch connection so that Experience Portal servers can communicate with each other, with any other speech servers, any application servers, and any Private Branch Exchange (PBX) servers.

Each server in your Experience Portal system must be able to connect to all the other servers in the system using the host names of the other servers. You must use a Domain Name Server (DNS) for this purpose.

Server name requirements

Each Experience Portal server must have a static IP address and a host name. Each host name must be unique and cannot contain a `.` (period) or a (space) character.

Site requirements

Verify that the site where you are installing the Experience Portal hardware platform is equipped with the following:

- Rack space for the servers that host Experience Portal.
- At least one network connection for each Experience Portal server. Depending on your network topology, two network connections might be required for each media server.
- Power supply.
- (Optional) Analog telephone line provisioned for Avaya Secure Access Link (SAL) or the Avaya Access Security Gateway (ASG) solution.

Chapter 6: Security

Security specification

The design of a self-service solution must include security considerations that are appropriate for your environment, to ensure:

- Sensitive customer data is not logged in plain text files
- Data is protected from unauthorized access and modification
- Applications do not inadvertently expose customer data
- Applications do not allow attackers access to the Private Branch Exchange (PBX)
- Machine operational status is not compromised through denial of service attacks

You can use the capabilities of the operating system or other custom-developed solutions to implement the required application-level security. Avaya realizes that many companies employ the use of third-party software to enhance system security. Avaya cannot ensure that such software does not affect the operation or performance capabilities of the Avaya Experience Portal system.

If you choose to install additional software, you must accept the responsibility of ensuring that it does not degrade system performance to an unacceptable level. Although you can choose to trade some system performance for the use of third-party applications, Avaya does not warrant that full system capacity be maintained. Furthermore, Avaya does not verify or ascertain the validity of third-party software unless prior business arrangements are made through Avaya. If you install additional software that causes problems on the system, Avaya might charge for any assistance required in troubleshooting the problem. Avaya might require that the software be removed before Avaya starts the troubleshooting process.

No telecommunications system can be entirely free from the risk of unauthorized use. You have the ultimate control over the configuration and use of the product and are solely responsible for ensuring system security. You can administer and tailor the system to meet your unique needs, and you are in the best position to ensure that the system is secure. You are responsible for keeping informed of the latest information, such as:

- Security patches
- Hot fixes
- Anti-virus updates

System managers and administrators are also responsible for reading all product recommendations, installation instructions, and system administration documents to understand the risks and to identify any preventative measures that they should take to keep their systems secure.

Avaya does not guarantee that this product is immune from or prevents unauthorized use of telecommunications services accessed through or connected to this product. Avaya is not responsible for any damages or charges that result from unauthorized use of this product. Avaya also is not responsible for incorrect installations of the security patches that are made available. To aid in combating unauthorized use, Avaya maintains strong relationships with its customers and supports law enforcement officials in apprehending and successfully prosecuting those responsible.

Report suspected security vulnerabilities with Avaya products by sending an email to securityalerts@avaya.com. Reported vulnerabilities are prioritized and investigated. Any corrective actions resulting from the vulnerability investigation are posted at the Avaya online security website, http://support.avaya.com/security.

Report all toll fraud incidents perpetrated on Avaya services to Avaya Corporate Security, to securityalerts@avaya.com, even if immediate support is required or not. In addition, for information concerning secure configuration of equipment and mitigation of toll fraud threats, see the *Avaya Toll Fraud and Security Handbook* at https://downloads.avaya.com/css/P8/documents/100171726 .

The Avaya Enterprise Security Practice, part of Avaya Network Consulting Services, can provide the following services to help protect against unanticipated threats and security hazards:

- Application assessment
- PBX assessment
- Network assessment
- Auditing
- Hardening services

For more information, or to contact the Avaya Enterprise Security Practice, call 1-866-832-0925.

If you want to perform the hardening steps, follow the steps described by the operating system manufacturer and security best practices. Security best practices are detailed in the National Security Agency Guides, http://www.nsa.gov/snac/.

In addition, to find related security advisories, report product vulnerabilities, and locate the latest software patches and upgrades, go to the Avaya online support Web site, http://support.avaya.com.

Secure system access

A key step in ensuring the security of a system is to the limit ways by which people can use the system. The following topics detail some of the ways you can limit access to Experience Portal:

- Physical system security
- Isolated LANs
- Firewalls

Physical system security

The Experience Portal system must be placed in a physically secure environment so that only a limited number of trusted people can use the system. Putting the system in a location that allows free access by anyone creates a risk that Experience Portal operation can be disrupted, whether unintentionally or maliciously. Isolate the Experience Portal system from everyone except trusted individuals.

Isolated LANs

Any server that is connected to the Internet is potentially subject to unauthorized use and malicious attacks. Experience Portal systems can be protected by configuring them on a LAN that has no physical connection to the Internet or to any internal unsecured networks. Sometimes referred to as an "island LAN," this type of network environment has its own LAN switch and contains only those network elements that the Experience Portal system needs to interface with. These elements include:

- Application servers
- Text-to-Speech (TTS) (TTS) and Automated Speech Recognition (ASR) servers
- Database servers, if used by the application
- PBX
- Backup server

If a LAN has no physical connection to the Internet, no risk of unauthorized access from external sources exist. As such, a firewall is not needed to protect the system from unauthorized use.

Physically isolating the LAN provides strong protection against fraudulent access. However, isolating the LAN can restrict the ability to remotely administer and maintain the Experience Portal system. Before deciding whether to place the Experience Portal system on an island LAN, you must consider the requirements of the operating environment.

Firewalls

If the LAN cannot be isolated, you can use firewall product to protect the LAN, and any Experience Portal servers connected to the LAN, from unauthorized access. The firewall should be installed on a machine that sits between the Internet and Experience Portal, so that all communication that comes into Experience Portal must first pass through the firewall.

A firewall also controls access of designated ports that use particular protocols or applications. They are commonly used to prevent the following:

- Denial of service attacks to application servers
- Snooping of sensitive data
- “Hijacking” access sessions that take control of a user session

  Session hijacking is the act of taking control of a user session after successfully obtaining or generating an authentication session ID. Session hijacking involves an attacker using captured, brute forced or reverse-engineered session IDs to seize control of a legitimate user's web application session while that session is still in progress.

Most firewalls can be configured to allow specified remote IP addresses to connect to designated ports by using specified protocols.

Even if a firewall protects the internal LAN, the Experience Portal system might still be accessible to unauthorized people who have access to the internal network. Therefore, you must still restrict access to the Experience Portal system in this environment to decrease the risk of fraudulent use by an insider.

Antivirus software

You can install antivirus software on the Experience Portal servers. The type of antivirus software used and the method of installation depends on the requirements of your company.

Make sure you use on-demand scanning, where scans are run at scheduled intervals. Do not use a message-scanning method, such as on-access scanning as that can impact the performance of Experience Portal. If your antivirus software runs whenever a file is changed, it can have a negative impact on Experience Portal performance.

In addition, some virus scan applications automatically start scanning at system startup by default. Disable this feature because it interferes with the time that it takes for an Experience Portal system to come back online after a reboot.

You must administer the antivirus software as follows:

- Scan the hard disk daily during off-peak hours, or at least once per week. Scans can be run on all Experience Portal servers simultaneously. Do not schedule the antivirus scan at the same time as a backup.
- Schedule antivirus definition updates to occur automatically at least once per week. The updates must occur before the next scheduled scan time to ensure that the latest data files are used during the scan. Do not schedule updates to occur during a virus scan.
- If the antivirus software detects a virus, it must attempt to clean the file. If the attempt fails, the software must move the infected file to a different directory on the server.

Network services

Experience Portal uses a few network services and several other services. Therefore, administrators disable the ports during the installation of Avaya Enterprise Linux as part of the bundled server offer.

Administrators enable the following network services while installing Avaya Enterprise Linux and Experience Portal:

- The Secure Shell (SSH) client that runs on all Experience Portal servers.
- Apache Tomcat that runs on the EPM server.

  Tomcat is a servlet container compliant with Jakarta Enterprise Edition (Jakarta EE), formerly known as Java 2 Platform, Enterprise Edition (J2EE). It is the default application server for the EPM.
- Network Time Protocol (NTP) that runs on all Experience Portal servers.
- PostgreSQL (SQL server) that runs on the EPM server.

  Postgres is an SQL-compliant, open source, and object-relational database management system for the Experience Portal database.
- Apache Hypertext Transfer Protocol (HTTP) daemon that runs on MPP servers.

MPP servers use Apache Web Server to implement web services for the following:

- EPM Monitoring and Control
- Media Server Service Menu

For more information about how Experience Portal protects sensitive data, see the Avaya Experience Portal Security White Paper in the *Print guides* section of the Avaya Experience Portal Documentation Library.

Secure Shell

Secure Shell (SSH) is a program that includes capabilities for doing the following:

- Logging in to another computer over a network
- Executing commands on a remote computer
- Moving files from one system to another

Secure Shell provides strong authentication and secure communications over untrusted networks. Secure Shell provides a more secure way to connect to remote systems than protocols such as telnet and FTP. Unlike telnet and FTP, users can connect to remote hosts over an encrypted link with SSH. Encryption protects against interception of clear text logins and passwords.

Network Time Protocol

If your Experience Portal system is configured to use a dedicated EPM server, and one or more dedicated MPP servers, Experience Portal uses Network Time Protocol (NTP) to synchronize the time between the EPM server and all other Experience Portal servers.

To do this, Experience Portal uses the chrony implementation. The Experience Portal software installer changes the /etc/chrony.conf file on each server on which the software is installed.

- When you install the Primary EPM software, the `chrony.conf` file on that server is set to point to the local clock.
- When you install the MPP software or the auxiliary EPM software, the `chrony.conf` file on that server is set to point to the primary EPM server as the reference clock.

Linux hardening

The general distribution of Red Hat Enterprise Linux includes the Red Hat Package Management (RPM) modules for most, if not all, possible Linux configurations. These distributions include a complete development suite, complete graphics support for the X Windows System, numerous development debugging tools and a variety of network administrative tools. For Experience Portal, only a small portion of the distributed RPMs is needed. When distributions of Red Hat Enterprise Linux grow to include more RPM modules, the relative percentage of RPMs needed by Avaya applications will be even smaller.

Experience Portal does not require most packages provided in the general distribution, and these unused RPMs are removed from the Avaya Enterprise Linux.

Aside from making the software product file images smaller and more manageable, the removal of unneeded RPM modules makes Linux more secure.

To make Linux even more secure, you must configure Linux to log security-related events, if possible. You must log the following events:

- Account privilege changes
- Logins and logouts
- System configuration changes
- Additions, modifications, or deletions of installed packages
- Activities of root or administrative logins

SNMP agents and traps

The Avaya Experience Portal Simple Network Management Protocol (SNMP) network includes agents, traps, and managers.

SNMP agents

You can configure Experience Portal to act as an *SNMP agent* so that a third-party network management software can retrieve the Experience Portal system status.

An SNMP agent is a software module that resides on a device, or node, in an SNMP-managed network. The SNMP agent collects and stores management information and makes this information available to *SNMP managers*. SNMP agent communication can be:

- Solicited by an SNMP manager.
- Initiated by the SNMP agent if a significant event occurs. This type of communication is called an *SNMP trap*.

The commands and queries that the SNMP agent can use, is stored in a Management Information Base (MIB) that resides on the managed device, along with the information about the target objects that the SNMP agent can interact with using these commands and queries.

SNMP traps

An SNMP trap is an unsolicited notification of a significant event from an SNMP agent to an SNMP manager. When an internal problem is detected, the SNMP agent immediately sends one of the traps defined in the MIB.

Important:

If you configure Experience Portal to send SNMP traps, you must configure the appropriate SNMP managers to receive the traps.

SNMP managers

SNMP managers collect information from SNMP agents. SNMP managers are usually used to display status information in a type of graphical user interface (GUI).

For Experience Portal, the SNMP manager can be an Avaya Services Security Gateway (SSG) or a Network Management System (NMS) station such as HP *OpenView* or IBM *Tivoli*. SNMP traps sent to the Avaya SSG contain specific information that generates Initialization and Administration System (INADS) notifications, which in turn generate customer trouble tickets.

Note:

You can only configure the Experience Portal SNMP agent and SNMP trap destinations if you are an administrator.

Transport Layer Security

Experience Portal provides TLS support for the following:

- EPM administration traffic runs over an TLS/HTTPS connection. Using an TLS/HTTPS connection ensures that no web administration data is transmitted in clear text. Encrypted data includes logins and passwords, configuration changes, and views of the Experience Portal system configuration.
- The EPM software must authenticate itself with the MPP before the MPP accepts any requests. Similarly, the MPP must authenticate itself with the EPM. All communication between the EPM and an MPP uses TLS/HTTPS.
- You can configure the Avaya Voice Browser to use TLS to access an application on the web server. In this case, VoiceXML data is transmitted in an encrypted format instead of clear text.

  Note:

  Although Experience Portal provides the framework for using TLS for VoiceXML, you must install an TLS certificate for each web server domain referenced by an application to fully implement client authentication using TLS for VoiceXML.

Avaya Secure Access Link (SAL) and Enhanced Access Security Gateway (EASG)

The EASG package is integrated into the Experience Portal system and provides secure authentication and auditing for all remote access into the maintenance ports.

EASG authentication is based on a challenge-response algorithm using a token-based, private key-pair cryptographic authentication scheme. Secure auditing is also provided in this challenge-response authentication and authorization solution. Logs include information such as successful log-ins, failed log-ins, errors, and exceptions.

With EASG, Avaya can control the access privileges of Avaya service engineers to customer products and permissions levels, such as init, inads, and craft.

In Experience Portal 8.0, a dedicated EASG Product Certificate is installed under the EASG directory `/etc/asg` on Experience Portal servers. It is mandatory that all Avaya products with EASG support, use the `/etc/asg` directory for all EASG associated files and directories. The EASG Product Certificate uniquely identifies Experience Portal 8.x major release to the Avaya EASG server. This is derived from the Avaya IT Root CA and intermediate CAs. The Avaya EASG server uses CAs to create a response, and Experience Portal uses the Experience Portal EASG Product Certificate Public Key to verify the response through the EASG Common RPM.

The site certificates are only used by on-site technicians who may not have access to connect to the EASG servers. Experience Portal supports the site certificates management through the EASG Common RPM.

Technical onboarding of Avaya Experience Portal 7.x and 8.x

For more information see, How to Register and Onboard Avaya Experience Portal on the Avaya Support website.

Technical onboarding of Avaya Solutions Platform 130 Series

For more information see Registering section and Avaya Technical Onboarding process section in *Installing the Avaya Solutions Platform 130 Series* guide on Avaya Support site http://support.avaya.com.

For more information on hardware references, see *Avaya Converged Platform 130 Series iDRAC9 Best Practices* guide on Avaya Support site http://support.avaya.com.

For more information on ASP platforms, see *Avaya Converged Platform overview and specification* guide on Avaya Support site http://support.avaya.com.

Port utilization

For complete port matrix information, see the Avaya Experience Portal Port Matrix on http://support.avaya.com.

Data transmission

When sending sensitive data from one place to another, use care because transmissions can be intercepted. Risks arise when transmitting data in clear text. Whenever you have the option, consider encrypting the data you are transmitting.

Data encryption

By design, communication between the EPM server and the MPP server is always encrypted. However, you have the option of enabling or disabling encryption for other types of data transmissions. Encrypting communication is more secure for your system, but keep in mind that encryption can slow system response times.

To encrypt the H.323/RTP media streams between an MPP and the PBX, use the encryption standard supported by the switch or gateway. In an Experience Portal system, Communication Manager supports the 128-bit Advanced Encryption Standard. After enabling encryption on the switch, you use the web interface to the EPM to enable encryption on Experience Portal.

Chapter 7: License requirements

License requirements

A license file is required for Avaya Experience Portal operation as it defines the features that are licensed for systems such as Telephony ports, the ASR and TTS connections, Email, HTML, and SMS units. The Avaya Experience Portal license file is distributed separately in an email from Avaya.

Use Web License Manager (WebLM) to manage the licensing of Experience Portal. WebLM is an integral part of the Experience Portal system that is available on the EPM server, and provides licenses to EPM. WebLM that resides on the EPM server is also referred to as Local WebLM. In most small setups of Experience Portal systems, the license is installed on the Local WebLM. An Enterprise or Master WebLM is used in a system that requires redundancy through a WebLM that is installed on a separate server. Enterprise WebLM allocates licenses to WebLM that resides on EPM. The location of Enterprise WebLM is critical to the facility of moving a license from one site to another in the event of a failure.

The Experience Portal Manager (EPM) contacts an Avaya WebLM server on a regular basis to determine the number of licenses that are authorized for your system. For security reasons, the license server must run WebLM 8.1 or later, and a valid Avaya Experience Portal Release 8 license must be installed on the license server. You must reinstall the license file while upgrading from a previous Experience Portal version that uses older WebLM versions.

After the EPM receives current information about authorized licenses, it allocates the available licenses among the servers in the system.

The licenses for outbound can be configured per zone because the telephony resources are also configured per zone.

Note:

The ASP 130 ESXi 6.5 software license key ownership is the customer responsibility.

The VMware ESXi license key is present on a label on the server cover. Losing the ESXi license key follows billable services recovery during server FRU replacement. During server recovery process, the customer needs to move the server lid including this label from the faulty server to the replacement server.

Chapter 8: Avaya AI Virtual Agent

Overview

Avaya has partnered its AI capabilities with Google Cloud Contact Center AI (CCAI) to seamlessly blend automated and assisted experiences into the customer journey.

Avaya has extended the capabilities of its contact center platforms to include an enhanced version of Google Cloud Dialogflow CX that can be used to create virtual agents infused with AI capabilities that verbally interact with customers.

Avaya AI Virtual Agent Enhanced is the newest co-innovation with Google Cloud. It provides new human-like automation features that significantly improve customer experience and contact center efficiency.

The powerful combination of Avaya AI innovation and Google Cloud CCAI seamlessly blends automated and assisted experiences throughout a customer's interaction with the contact center to provide a better user experience.

Proof of Concept (PoC)

The Avaya Evaluation Agreement is a legal agreement between Avaya and a Customer for evaluating Avaya CCAI. Avaya provides the customer an opportunity to test Avaya CCAI free of charge for 30 days.

At the end of the 30-day evaluation, customer access to the CCAI service is disabled. If the customer wants to purchase the CCAI service, the customer must contact the Avaya sales team.

To ensure a successful and safe evaluation, the customer must note the following:

- Avaya provides the services for testing and evaluation purposes only. The services are not to be used in a production/live environment.
- Avaya provides the services "as is", "as available", and with no warranty of any kind.
- The use of the services is in accordance with the CCAI Service Description mentioned in the *Support Services Policies & Customer Services Description* section on the Avaya Support website at https://support.avaya.com/helpcenter/, which may be updated from time to time.

Note:

The processing of customer personal data is in accordance with the Data Processing Addendum on the Avaya Support website at http://support.avaya.com/TermsOfSale, which may be updated from time to time.

Filling the Avaya Evaluation Agreement form

About this task

The customer must sign the evaluation agreement Avaya sends to acknowledge the customer's agreement with the terms of the evaluation and to ensure a successful evaluation period.

Procedure

1. Fill in the required information in all the highlighted fields in the agreement.

   After you fill in the required information, ensure that you remove highlighting from the document.

2. Sign your name above the signature block to acknowledge your agreement with the letter and the terms of the evaluation.

3. Forward a copy to the NPI Operations team.

4. Contact your assigned contract negotiator if you have any questions.

Provision Google CCAI with Avaya Experience Portal

This section describes how to provision Google Contact Center Artificial Intelligence (CCAI) with Avaya Experience Portal (AEP).

AEP customers can leverage Virtual Assist and Conversational Interactive Voice Response (IVR) capabilities powered by Google CCAI. This section outlines the steps partners or customers must follow to enable Google CCAI services procured through Avaya and provision it to work with AEP.

Onboarding a customer GCP project

About this task

When the customer places an order, A1S sends an email to Avaya Sales. The email contains Google CCAI material codes for a new project.

The following procedure details the steps the Avaya Sales Account Manager must perform to onboard a customer GCP project.

Procedure

1. Enter the appropriate information in the General Information tab of the Onboarding Information Worksheet.

2. Email the Onboarding Information Worksheet to the customer.

The customer fills in the GCP project ID and the authorized email addresses to download the GCP service account key file and sends the worksheet back to the NPI Operations and Sales teams.

3. Onboard the customer GCP project.
4. Enter the service account ID and key file URL in the Onboarding Information Worksheet.

   Note:

   The Avaya service account is used to track customer billing.

5. Send the Onboarding Information Worksheet back to the customer.

   The NPI Operations team sends the worksheet to the authorized email handles mentioned in the Onboarding Information Worksheet.

Avaya AI Virtual Agent Onboarding Information Worksheet

There are two tabs on the Onboarding Information Worksheet:

- General Information tab: To be completed by the Avaya Sales Account Manager.
- Sample BOT tabs: To be completed by the customer.

Note:

The worksheet has multiple sample tabs, such as the Customer Service Bot, FAQ Bot, and Tech Support Bot tabs. If the customer has more than one Bot, the customer must fill in one tab for each Bot.

Avaya AI Virtual Agent Onboarding Information Worksheet field descriptions

General Information tab

Name	Description
Purchase Order Number	The unique number assigned to the purchase order.
End Customer Name	The name of the end customer.
End Customer Sold To	The address of the end customer.

Sample BOT tab

Customer Information on a BOT tab (Completed by the customer):

The green and yellow sections on the worksheet are populated with customer information.

Name	Description
Customer Name	The name of the end customer.

Table continues…

Name	Description
CI/CD Stage Name (E.g. prod, dev, uat)	The number and names of CI/CD stages used by the customer CI/CD process for the Customer Project Name. The CI/CD Stage Name identifies the customer's GCP project as Production, UAT, or Test. All bots under the same GCP project will have their usage tracked as a single entity by GCP. Avaya will be unable to provide break-down information. One service account is created for each CI/CD stage of each bot.
Customer GCP Project ID	The Google Cloud Platform (GCP) project ID for each project created by the customer to host CCAI resources. For example, Dialogflow agent.
Authorized Email Handles for the JSON Key File	The email addresses authorized to download the Avaya GCP Service Account key file. The access automatically expires after 30 days. All email addresses must be registered Google accounts. ✱ **Note:** If enterprise security does not enable a Google account creation, a Gmail account can be used. However, the customer must verify if this is acceptable according to their enterprise security policies.
Google Workspace/Cloud Identity Group	The groups created and managed by the customer in Gsuite or Cloud Identity. Using these groups, the customer can access resources such as reporting dashboards and quota information. ✱ **Note:** This field is not required to set up the CCAI projects for onboarding. However, it is necessary to access the CCAI Usage Dashboard that the customer can use to view transactions.

Avaya Information on a BOT tab (Completed by Avaya):

The NPI Operations team adds the service account and key file information in the blue sections of the worksheet and sends the worksheet back to the customer.

Name	Description
Creation Date	The date the service account and key file are created.
Avaya GCP Service Account	The Avaya GCP service account which must be assigned `IAM role = Dialogflow API Admin` in the corresponding customer's GCP project.

Table continues…

Name	Description
Avaya GCP Service Account JSON Key Link	The URL from which the users mentioned in the **Authorized Email Handles** field can download the Avaya GCP service account JSON key file. The key file is used to provision CCAI services consumed by Avaya components. **Note:** The key file is available for download for 30 days from the creation date.

Checklist for provisioning Google CCAI with Avaya Experience Portal - Initial onboarding

The following checklist details the steps the customer must perform during the initial onboarding:

No.	Task	Description	✔
1	Place an order on Avaya One Source (A1S).	Customers and partners can log in to A1S and place an order for Google CCAI.	
2	Complete the Onboarding Information Worksheet sent by Avaya.	There are two tabs on the Onboarding Information Worksheet: • General Information tab: Completed by the Avaya Sales Account Manager. • Sample BOT tabs: Completed by the customer. See: • Avaya AI Virtual Agent Onboarding Information Worksheet on page 75 • Avaya AI Virtual Agent Onboarding Information Worksheet field descriptions on page 75	
3	Send the Onboarding Information Worksheet to the NPI Operations team to obtain a CCAI service account and key file.	After the customer fills in the required information in the Onboarding Information Worksheet, the customer sends the worksheet back to the NPI Operations and Sales teams. The NPI Operations team creates service accounts and its corresponding key files. This information is added to the Onboarding Information Worksheet and returned to the customer.	

Table continues…

No.	Task	Description	✔
4	Authorize the Avaya-provided service account on the customer GCP project.	The customer must authorize the Avaya Service Account in their GCP project. See: • Authorizing the Avaya-provided service account on the customer GCP project on page 78 • Configuring the Avaya-provided service account in Avaya Experience Portal on page 78	

Authorizing the Avaya-provided service account on the customer GCP project

About this task

The customer must authorize the Avaya Service Account in their GCP project.

Use this procedure to authorize the Avaya-provided service account with the customer GCP project from the GCP console.

Procedure

1. Login to the GCP console.
2. On the dashboard, click **Select a project** and select a GCP project ID specified on the onboarding worksheet.
3. On the left navigation pane, click **IAM & Admin** > **IAM**.
4. Click **+ADD**.
5. In the **New Members** field, enter the name of the new member and the corresponding Avaya GCP Service Account from the onboarding worksheet.
6. In the **Role** field, set the role to **Dialogflow API Admin**.
7. Click **Save**.

Configuring the Avaya-provided service account in Avaya Experience Portal

About this task

The customer must configure the Avaya Service Account in Avaya Experience Portal.

Use this procedure to configure the Avaya-provided service account in Avaya Experience Portal.

Procedure

1. Go to https://accounts.google.com/.

2. Sign in using the Google Account email specified in the Onboarding Information Worksheet.
3. Open the Onboarding Information Worksheet and do the following:
    a. Click the BOT tab.
    b. In the **Avaya GCP Service Account JSON Key Link** field, click the key file link.
4. Download the key file and save it on your computer.
5. Log in to Avaya Experience Portal.
6. Enter the appropriate details in the following fields:
    - **Project ID**: Enter the **Customer GCP Project ID** from the Onboarding Information Worksheet.
    - **Credentials**: Enter the JSON key file that you downloaded.

Checklist for provisioning Google CCAI with Avaya Experience Portal - subsequent GCP projects

The following checklist details the steps the customer must perform for the subsequent GCP projects:

No.	Task	Description	✔
1	Select the order on Avaya One Source (A1S).	Customers and partners can log in to A1S and select the order for Google CCAI.	
2	Complete the Onboarding Information Worksheet sent by Avaya.	There are two tabs on the Onboarding Information Worksheet: • General Information tab: Completed by the Avaya Sales Account Manager. • Sample BOT tabs: Completed by the customer. See: • Avaya AI Virtual Agent Onboarding Information Worksheet on page 75 • Avaya AI Virtual Agent Onboarding Information Worksheet field descriptions on page 75	

Table continues…

No.	Task	Description	✔
3	Send the Onboarding Information Worksheet to the NPI Operations team to obtain a CCAI service account and key file.	After the customer fills in the required information in the Onboarding Information Worksheet, the customer sends the worksheet back to the NPI Operations and Sales teams. The NPI Operations team creates service accounts and its corresponding key files. This information is added to the Onboarding Information Worksheet and returned to the customer.	
4	Authorize the Avaya-provided service account on the customer GCP project.	The customer must link their GCP project to the Avaya Service Account. See: • Authorizing the Avaya-provided service account on the customer GCP project on page 78 • Configuring the Avaya-provided service account in Avaya Experience Portal on page 78	

Avaya Invoice breakdown

Customers receive an invoice from Avaya at the end of the billing period. The invoice contains an itemized list of the products or services provided to the customer with the unit price, quantity, and total price for each item. In addition to a description of the products or services provided, the invoice states the total amount due, the due date for payment, and sets up payment terms for the transaction.

Submitting a billing dispute

About this task

If customers have questions or issues regarding the invoice, customers can submit a billing dispute through the Avaya OneCare portal.

Procedure

1. Sign in to onecare.avaya.com.
2. In the **View** field, select **Partner Support**.
3. Click **Invoice and Dispute Management**.
4. Enter the appropriate information and click **Submit**.

Chapter 9: Resources

Documentation

The following table lists the documents related to Avaya Experience Portal. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Avaya Experience Portal Documentation Roadmap	Lists all the documents related to Experience Portal and describes the organization of content across the documents.	Avaya Professional Services Implementation engineers
Administering Avaya Experience Portal	Provides general information about and procedures for administering and configuring specific Experience Portal functions and features using a web-based interface.	Administrators Implementation engineers
Avaya Experience Portal Overview and Specification	Describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	Administrators Sales engineers Implementation engineers Avaya Professional Services
Implementing Avaya Experience Portal on a single server	Provides procedures to install and configure the Avaya Experience Portal software on a single server.	Implementation engineers
Implementing Avaya Experience Portal on multiple servers	Provides procedures to install and configure Avaya Experience Portal software on two or more dedicated servers.	Implementation engineers

Table continues…

Title	Description	Audience
Deploying Avaya Experience Portal in an Avaya Customer Experience Virtualized Environment	Provides procedures for deploying the Experience Portal virtual application in the Avaya Customer Experience Virtualized Environment. This document includes installation, configuration, initial administration, troubleshooting, and basic maintenance checklists and procedures.	Implementation engineers
Upgrading to Avaya Experience Portal 8.1	Describes how to upgrade your Avaya Experience Portal system to Avaya Experience Portal 8.1.	Implementation engineers
Troubleshooting Avaya Experience Portal	Provides general information about troubleshooting and resolving system problems. This document also provides detailed information and procedures for finding and resolving specific problems.	Administrators Implementation engineers Avaya Professional Services
Avaya Experience Portal Solutions Guide	Provides a high-level description of Avaya Experience Portal as well as topology diagrams, connectivity details, interoperability concept, product interactions, and failover best practices.	Sales engineers Implementation engineers Avaya Professional Services
Avaya Experience Portal Programmer's Reference	Provides information about designing speech applications for Avaya Experience Portal.	Application Developers
Deploying Avaya Experience Portal on Amazon Web Services	Provides procedures for deploying Avaya Experience Portal as *Software as a Solution* by using the Amazon Web Services Management console.	Administrators Implementation engineers Support Personnel Avaya Professional Services
Deploying Avaya Experience Portal on Google Cloud Platform	Provides procedures for deploying Avaya Experience Portal as *Software as a Solution* by using the Google Cloud Platform.	Administrators Avaya Professional Services Implementation engineers Support Personnel

Table continues…

Title	Description	Audience
Deploying Avaya Experience Portal on Microsoft Azure	Provides procedures for deploying Avaya Experience Portal as *Software as a Solution* by using the Microsoft Azure portal.	Administrators Implementation engineers Support Personnel Avaya Professional Services
Avaya Experience Portal Security White Paper	Provides information about the security strategy for Experience Portal, and provides suggestions that companies can use to improve the security of the Experience Portal systems and applications.	Avaya Professional Services Implementation engineers
Avaya Experience Portal Mobile Web Best Practices White Paper	Provides recommended strategies for deploying Avaya Orchestration Designer Mobile Web applications with Avaya Experience Portal, detailing configuration for security, scalability and high availability.	Avaya Professional Services Implementation engineers
Avaya Experience Portal Call Classifications White Paper	Provides information about the call classification feature in Avaya Experience Portal, detailing the configuration and tuning of the call progress engine.	Sales engineers Implementation engineers
Avaya Experience Portal Dialogflow White Paper	Provides information about connecting Avaya Experience Portal self-service applications to Google Dialogflow. This document provides details on configuration, licensing, and other information to help customers with Dialogflow integration.	Avaya Professional Services Implementation engineers
Avaya Experience Portal Nuance Mix Integration White Paper	Provides information about connecting Avaya Experience Portal to Nuance Mix. This document provides details on configuration, licensing, and other information to help customers with Nuance Mix integration.	Avaya Professional Services Implementation engineers

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.

2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click 🔍 to display the search results.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** (🌐) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.

- Click **Share** (➦) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** (🔖). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.
- Click **Watch** (👁) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After logging in to the website, enter the course code or the course title in the **Search** field and press **Enter** or click **>** to search for the course.

Course code	Course title
20641W	Administering Avaya Experience Portal R8
70051V	Implementing and Supporting Avaya Experience Portal and Proactive Outreach Manager
7006W	Implementing and Supporting Avaya Intelligent Customer Routing
20931W	Administering Avaya Proactive Outreach Manager R4
25101V	Creating Self Service Apps with Avaya Orchestration Designer

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

  Note:

  Videos are not available for all products.

Policies for technical support of the Avaya Solutions Platform (ASP) 130

For more information on ASP 130, see Policies for technical support of the Avaya Solutions Platform (ASP) 130 on the Avaya Support site.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Warranty

Avaya provides a 90-day limited warranty on Avaya Experience Portal. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation.

In addition, the Avaya standard warranty description and details for support under warranty are available on the Avaya Support website.

Glossary

Application server

A server that runs in conjunction with a Web server and allows client programs, such as Avaya Agent Web client, to call methods over HTTP.

Avaya Aura®

A converged communications platform unifying media, modes, network, devices, applications. Avaya Aura® is based on the SIP architecture with Session Manager at the core.

Communication Manager

A key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media gateways and analog, digital, and IP-based communication devices. It includes advanced mobility features, built-in conference calling, contact center applications and E911 capabilities.

EASG

Enhanced Access Security Gateway (EASG). The EASG package is integrated into the Experience Portal system and provides secure authentication and auditing for all remote access into the maintenance ports.

EPM

Experience Portal Manager is the Web interface used to access Experience Portal.

IVR

Interactive voice response (IVR) automates interactions with telephone callers.

Session Manager

An enterprise SIP proxy registrar and router that is the core component within the Avaya Aura® solution.

SIP

Session Initiation Protocol (SIP) is an application-layer control signaling protocol for creating, modifying, and terminating sessions with more than one participant using http like text messages.

TCP

Transmission Control Protocol is one of the core protocols of Internet Protocol Suite, the set of network protocols used for the Internet.

Telephony ports

Ports that represent the telephony hardware. For example, if you use one PRI, you have 23 telephony ports available for inbound and outbound calls.

TLS

Transport Layer Security (TLS) is a cryptographic protocol that provide communication security over the Internet.

Index