Avaya Aura® Experience Portal Overview and Specification

Release 7.0
Issue 1
December 2013

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

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

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

License types

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Copyright

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

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/

Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document describes tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.

Intended audience

This document is intended for anyone who wants to gain a high-level understanding of the product features, functions, capacities, and limitations within the context of solutions and verified reference configurations.

Related resources

Documentation

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

Title	Description	Audience
Implementing Avaya Aura® Experience Portal on multiple servers	Provides procedures to install and configure Avaya Aura® Experience Portal software on two or more dedicated servers.	Implementation engineers
Implementing Avaya Aura® Experience Portal on a single server	Provides procedures to install and configure the Avaya Aura® Experience Portal software on a single server.	Implementation engineers

Title	Description	Audience
Upgrading to Avaya Aura® Experience Portal 7.0	Provides procedures to upgrade the Voice Portal 5.1 server or Avaya Aura® Experience Portal 6.0.x server to Avaya Aura® Experience Portal 7.0.	Implementation engineers
Deploying Avaya Aura® 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
Avaya Aura® 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 theExperience Portal systems and applications.	Avaya Professional Services Implementation engineers

Training

The following traditional courses are transitioning into the Avaya Learning virtual campus and will eventually be retired.

Course code	Course title
4C00101W	Avaya Aura® Experience Portal Administration.
5C00092I/V	EP, OD, POM Install, Maintenance and Troubleshooting
V: Virtual I: Classroom Instructor led W: Self-Paced Web	

For details on the traditional curriculum and the new virtual campus offerings course descriptions, pricing, and registration, go to Avaya Learning website at www.avaya-learning.com.

Avaya Learning Virtual Campus technical training offerings:

Avaya Learning Virtual Campus helps simplify and speed how partners and customers train, learn, and complete credentials for Avaya solutions.

Users can interact with others in a virtual environment using avatars, spatial audio, and unique collaboration tools.

Course details:

- 5C00040E – Knowledge Access: ACSS Avaya Aura Experience Portal with Proactive Outreach Manager
  - Self-Directed content available 24/7
  - Hands-on Labs in virtual environment – scheduled sessions

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 http://support.avaya.com, select the product name, and check the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

Visit the Avaya Support website at http://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 Aura® Experience Portal. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation.

In addition, Avaya's standard warranty description and details for support under warranty are available on the Avaya Support website at **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. Also see **Help & Policies** > **Policies & Legal** > **License Terms**.

Chapter 2: Experience Portal overview

Avaya Aura® Experience Portal provides a single platform for automated voice and multimedia, self service, and Interactive Voice Response (IVR) applications. Experience Portal supports inbound phone, video, SMS, and email applications. Experience Portal also supports outbound phone, SMS, and email applications.

Use Experience Portal to employ self-service treatments with the following key features:

- Intelligent Customer Routing (ICR) for enhanced wait treatment and load balancing
- Proactive Outreach Manager (POM) for outbound phone, email, and SMS campaigns

Experience Portal supports SIP, H.323, and mixed telephony environments.

Configuration options

When you install the Experience Portal software, you can use a single server or multiple servers, depending on the number of telephony ports required.

- Single server configuration: This configuration includes a single server running both the Experience Portal Manager (EPM) and Media Processing Platform (MPP) software. The single server configuration can be deployed with an optional co-resident application server.
- Multiple server configuration: This configuration includes two or more servers, one dedicated to running the primary EPM software and at least one dedicated to the MPP software. In addition, you can have an auxiliary EPM server that handles failover for Application Interface web service requests.

New in this release

Avaya Aura® Experience Portal 7.0 offers the following new capabilities:

- 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, 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 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 Avaya Aura® Experience Portal in the Avaya Customer Experience Virtualized Environment. The Avaya Aura® Experience Portal virtualized environment offer consists of the following three OVA files:
  - Primary EPM
  - Auxiliary EPM
  - MPP

Feature Description

Experience Portal provides the following software elements:

- Media server software that provides IVR-based functionality.
- Experience Portal Manager application that offers centralized management for Experience Portal, POM, and ICR.
- Web Server host that provides the standards-based VoiceXML, CCXML, or TextXML script to the media server.
- Orchestration Designer tool that you can use to build speech applications, call control applications, and message applications. You can deploy the VXML or CCXML applications on an existing Apache Tomcat, IBM WebSphere, or Oracle WebLogic Web server environment. You can also deploy TextXML-based applications which are developed with Orchestration Designer.

- Avaya Aura® Orchestration Designer (OD) supports application development for Experience Portal.
- Call Classification.

Experience Portal media servers

Experience Portal supports the Media Processing Platform (MPP) media server.

Media servers provide automation functionality such as:

- Terminating telephony sessions
- Interfacing to third-party speech and other multimedia service
- Managing VoiceXML and CCXML sessions
- Supporting control of multiple voice dialogs and sessions and advanced call control functions with a fully programmable CCXML Session Manager.

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

Experience Portal Manager

Experience Portal Manager provides centralized operation, administration, management, and provisioning interface for Experience Portal, ICR, POM, and other Avaya and Avaya Partner applications. An easy-to-use, Web-based interface provides support for the following:

- Media servers that support all concurrent self-service sessions across your enterprise, including Email and SMS
- 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

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 user name dictates which pages the user can see and what actions the user can perform.
- Sends relevant configuration information to each MPP server.
- Routes outgoing calls made with the Application Interface web service to an available MPP server.
- Collects the operational status from each MPP server and displays it on the EPM Web interface.
- Monitors the heartbeat of the MPP servers and redistributes telephony ports when an MPP fails.
- Receives event and alarm messages from all MPP servers.
- Downloads report data from all MPP servers and stores it in the Experience Portal database so that users can create reports that contain information from all MPP servers in the system.
- Interacts with the Avaya WebLMlicense server to distribute and manage Automatic Speech Recognition (ASR), Text-to-Speech (TTS), and Telephony ports across all MPP servers.
- Provides an optional Simple Network Management Protocol (SNMP) interface to monitor Experience Portal alerts.
- Handles Application Logging web service 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.

- 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.

Directory details of the EPM system components

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

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

Standard RHEL packages that might be installed with or used by Experience Portal, such as Apache and NTP, are not included in this list.

Component	Directory
Experience Portal Manager web application	/opt/Tomcat/tomcat/webapps/VoicePortal
Avaya Aura® Experience Portal Management web services	/opt/Tomcat/tomcat/webapps/axis2
Application log manager	/opt/Tomcat/tomcat/webapps/axis
Alarm manager	/opt/Tomcat/tomcat/webapps/axis
Network log manager	/opt/Tomcat/tomcat/webapps/axis
Avaya License Manager	The co-located WebLM is installed in the /opt/Tomcat/tomcat/webapps/WebLM directory. **Note:** If you use an external WebLM, the license manager may be installed in a different directory on the external system.
Experience Portal database	The Postgres files are installed in the /var/lib/pgsql directory. **Note:** Most of the database data is in the /var/lib/pgsql/data directory.
Java	/usr/java
Tomcat for EPM	/opt/Tomcat
Tomcat for SMS and Email Processor	/opt/MMSServer
Apache Axis: web services container	/opt/Tomcat/tomcat/webapps/axis
Apache Axis2: Web services container	/opt/Tomcat/tomcat/webapps/axis2

Component	Directory
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

EPM components

Installed on the Linux operating system, the EPM software 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

Additionally, the EPM relies on several third-party components, which are installed automatically as part of the EPM installation, including:

- Java, Standard Edition Software Development Kit: Java run-time environment
- Apache Tomcat: web servlet container
- Apache Axis: web services 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 Web pages 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 the Avaya License Manager

Application log manager

The application log manager receives log entries generated by applications developed by using 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. When appropriate, the alarm manager generates an alarm.

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 Telephony ports, Automatic Speech Recognition (ASR), and Text-to-Speech (TTS) resources that you have purchased. Experience Portal must be able to communicate with the WebLM server in order to process any incoming or outgoing calls.

The WebLM server software is automatically installed with the Experience Portal primary EPM software, but you can also connect your Experience Portal 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 both the EPM and the media servers.

Because the database is located on the EPM server, the MPP servers do not need to be backed up.

Note:

You should not modify the Experience Portal internal database. For assistance to modify the database, contact your Avaya technical support representative.

Application Execution Environment

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

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

Multichannel components

To support SMS and Email, Experience Portal provides the following components:

- SMS Web 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 OD applications for outbound SMS messages.
- Email Web 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 that interface to the external client and send SMS and email messages.

Avaya Aura® Orchestration Designer

Orchestration Designer (OD) is a tool that you can use to build speech applications, call control applications, and message applications. You can deploy the VXML or CCXML applications on an existing Apache Tomcat, IBM WebSphere, or Oracle WebLogic Web server environment. You can also deploy the textXML applications that are developed with OD. You must use OD to write SMS and Email applications in Experience Portal.

OD is available at no added cost with every Experience Portal purchase and is downloadable from Avaya DevConnect on http:// www.Avaya.com.

Proactive Outreach Manager (POM)

POM is a managed application of Avaya Aura® 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.

Intelligent Customer Routing (ICR)

ICR provides features to efficiently handle customer calls. With ICR, calls are either completely served through self service applications or intelligently routed to a relevant call center across applicable geographic locations based on the best available source of real-time data.

ICR provides the following features:

- Self service first using Experience Portal as the first point of access to an organization.
- Intelligent routing of calls.
- Enhanced or advanced wait treatment such as self service or predictive offers to callers.

Call classification

Experience Portal 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

Zoning

Zoning is the capacity of partitioning a system into multiple zones.

This feature provides an advantage to customers at geographically distributed sites and to customers that have a large system in a single location.

Zoning entails three main advantages for Experience Portal customers:

- Easy management of large systems, such as MPPs
- Effective management of WAN traffic
- Local Access and Transport Area (LATA) considerations for outbound calls

Zone architecture

Zones are extended Experience Portal systems. All resource management and configuration are centralized in zones. Each zone is either co-resident 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. All primary EPM data traffic crosses zonal boundaries including configuration information, control, status information, and report data. SIP traffic can also cross zonal boundaries though each zone must have a configured proxy.

The zone specific resources are:

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

Note:

The proxies are shared across zones but traffic routing causes certain issues. The shared proxies provide 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.

Resource management and licensing

Resource management in Experience Portal is done in three levels:

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

The licenses are manually assigned to each zone by the Experience Portal administrator 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 even if there are unused licenses available in other zones. The administrator must control the resource allocation to zones effectively, so that each zone gets the required number of licenses.

Moving resources between zones

The 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 coresident SMS processor uses SMPP Connection that 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	All media servers are stopped in the zone from which the resource is being moved.
H.323 Connections	All media servers are stopped in the zone from which the resource is being moved.
SIP Connections	All media servers are stopped in the zone from which the resource is being moved.

Resource	Restrictions
SMPP connections	All auxiliary EPM servers must be stopped in the zone from which the resource is being moved.
HTTP connections	All auxiliary EPM servers must be stopped in the zone from which the resource is being moved.
Email Connections	All auxiliary EPM servers must be stopped in the zone from which the resource is being moved.

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

Experience Portal supports Red Hat Enterprise Linux Release 6.4 64 bit or later and Avaya Enterprise Linux RH6.4.64-AV13EP7 or later.

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

Orchestration Designer requirements

To create applications with Orchestration Designer, select one of the following application servers:

- Apache Tomcat
- IBM WebSphere Application Server (WAS)
- IBM WebSphere Express
- BEA WebLogic

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

Development Environment (IDE), Service Creation Environment desktop and laptop specification

For a 1-GHz desktop or laptop, you require the following components:

- Minimum 512K RAM
- Minimum 40-GB disk space
- Windows XP or Windows 2000 professional

Enhanced Basic Speech is available in Orchestration Designer as Audio variables within the phrase or prompt editors. The Audio variables include numbers in various formats, currency words, and names of months and days. See *Orchestration Designer Developers' Guide* for the languages supported by Orchestration Designer.

Cleo 3270/5250 Transaction Processor 5.x.5 integration using Web services

Experience Portalsupports FAX tone. You can integrate external fax servers with Orchestration Designer to support the fax-back functionality. For example, Orchestration Designer can integrate with Fax Services through Java or Web Services integrations. A number of third-party FAX servers integrate well with Orchestration Designer. For example, RightFAX and Biscom.

The connectors included with Orchestration Designer are as follows:

- Java
- Web Server (WS)
- Database (DB) JDBC SQL used to access remote databases
- Interaction Center (IC)
- CTI used for outbound dialing

Third-party product requirements

In the Experience Portal network, external systems include Speech servers, Email servers, SMS servers, and Application servers.

Related topics:

External database requirements on page 25
Speech application requirements on page 25
Application server requirements on page 26
Application Logging web service on page 27
Text application requirements on page 28
Speech server requirements on page 28
SIP requirements on page 30
H.323 requirements on page 30
Feature Comparison between H.323 and SIP on page 31
Minimum server machine hardware requirements on page 34
PBX requirements on page 35
LAN requirements on page 35
Site requirements on page 36

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:

- Postgres 9.2.x
- Oracle 10 and 11g
- Microsoft SQL Server 2008, 2010, and 2012

For more information on external databases, see *Administering Avaya Aura® Experience Portal*.

Speech application requirements

The following technologies are required for Experience Portal speech applications:

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.

Related topics:

Speech application development tools on page 26

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 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 thrid-party products.

Related topics:

Dedicated server requirements on page 27
Single server requirements on page 27

Additional information on page 27

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 6.0.x
- Java version 1.7, which is automatically installed when you install the Avaya Aura® Experience Portal software

Note:

Avaya Aura® Experience Portal includes an installation script for the Tomcat 6.0.37 application server. If you select any other version of Tomcat, you must manually install the Application server.

Additional information

For more information about:

- Java, go to http://java.sun.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 7.0.

Text application requirements

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

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 the Orchestration Designer tool meet these requirements and recommendations.

Speech server requirements

If your speech applications require Automatic Speech Recognition (ASR) or Text-to-Speech (TTS) resources, you must purchase and install one or more of the following 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:

You must purchase the recommended versions of ASR and TTS from the vendors, and use the matrix mentioned in this section to install the correlated components.

Supported speech server versions for ASR and TTS

Speech Server	Components	Minimum version	Recommended version
Nuance 9	Nuance Speech Server (NSS)	5.1.3	5.1.9
	Recognizer	9.0.12	9.0.19
	Vocalizer	5.0.3	5.0.7
Nuance 10	Nuance Speech Server (NSS)	6.2.0	6.2.4
	Recognizer	10.2.0	10.2.4
	Vocalizer	5.7.0	5.7.3
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 7.10.1 + patch 3
	TTS	See recommended version	LTTS 7.25.2 + patch 1
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

Speech Server	MRCP v1 Support	MRCP v2 Support
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 version 5.2 with Communication Manager version 5.2 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 5.2 or later.

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

You must use Communication Manager 5.2.1 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 a Communication Manager version earlier than 5.2.1. Communication Manager 5.2.1, provides the SA8874 Green Feature. However, you must turn the feature on for implementation.

Feature Comparison between H.323 and SIP

This table compares:

- Standard H.323
- H.323 with the Avaya Special Application SA8874 feature enabled in Communication Manager
- SIP

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	Operates like a blind transfer.	Supported	Supported

Feature	H.323	H.323 with SA8874 feature	SIP
consultative transfer) **Note:** If a connection cannot be established, use the Consultative Transfer feature in Experience Portal to allow the application to regain control of the call.	**Note:** The only supported VoiceXML event for this transfer is `error.connection.noroute`.		
Bridge transfer. See also Bridge transfers in a mixed SIP or H.323 environment on page 34	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 **Note:** Experience Portal supports only out-band DTMF detection.	Supported	Supported	Supported **Note:** 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

Feature	H.323	H.323 with SA8874 feature	SIP
Encryption options	• Disabled • Advanced Encryption Standard (AES) • Avaya™ Encryption Algorithm (AEA)	• Disabled • AES • AEA	• Disabled • TLS • SRTP
Quality of Service	Supported	Supported	Supported
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. **Note:** 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.	Supports the capability to receive UCID over H323 from Communication Manager. **Note:** 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.	Supports the capability to both send and receive UCID. **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.	An alternate gatekeeper address can be specified in the EPM. Communication Manager can supply an alternate	Experience Portal does not supply additional support, but the Avaya Aura® Session Manager hardware has failover support and MPPs can be configured as

Feature	H.323	H.323 with SA8874 feature	SIP
		gatekeeper address list.	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 and get a SIP outbound channel.

Minimum server machine hardware requirements

Customer supplied servers must meet the following minimum specifications in order to run Avaya Aura® 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 ASG solution. If you purchase a maintenance agreement with Avaya Services, the Experience Portal system requires SAL or Avaya ASG solution so that Avaya Services can remotely access the system for maintenance purposes. Contact Avaya Support to determine the version of SAL and Avaya ASG 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 5.2 or later
H.323 with supervised transfer or the Application Interface web service for outbound calls	Communication Manager 5.2 with the Avaya Special Application SA8874 feature
SIP	Avaya Aura® Session Manager version 5.2 or later with either Communication Manager version 5.2, a third-party SIP Gateway, or SIP Trunk
SIP with SRTP	Avaya Aura® Session Manager version 5.2 or later with Communication Manager version 5.2

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
Calls (Standalone media server)	Up to 1,000 simultaneous calls[1]
Inbound calls	Up to 1,000 simultaneous calls[1]
Outbound calls	Up to 1,000 simultaneous calls[1]
Calls (Single-Box system)	Up to 350 simultaneous calls[1]
Inbound calls	Up to 350 simultaneous calls[1]
Outbound calls	Up to 350 simultaneous calls[1]

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			
Outbound only	Up to 25,000[2] [3]	Up to 50,000[2] [3]	Up to 5,000[2] [3]
Inbound only	Up to 12,500[2] [3]	Up to 25,000[2] [3]	Up to 2,500[2] [3]
SMS Messages			
Outbound only	Up to 25,000[2]	Up to 50,000[2]	Up to 5,000[2]
Inbound only	Up to 12,500[2]	Up to 25,000[2]	Up to 2,500[2]

[1] Varies based on application complexity, audio codex, 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.

Traffic specification

Network topology

Partitioning your Experience Portal network increases the available network bandwidth.

- Experience Portal physical server HP Proliant DL360 G7 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

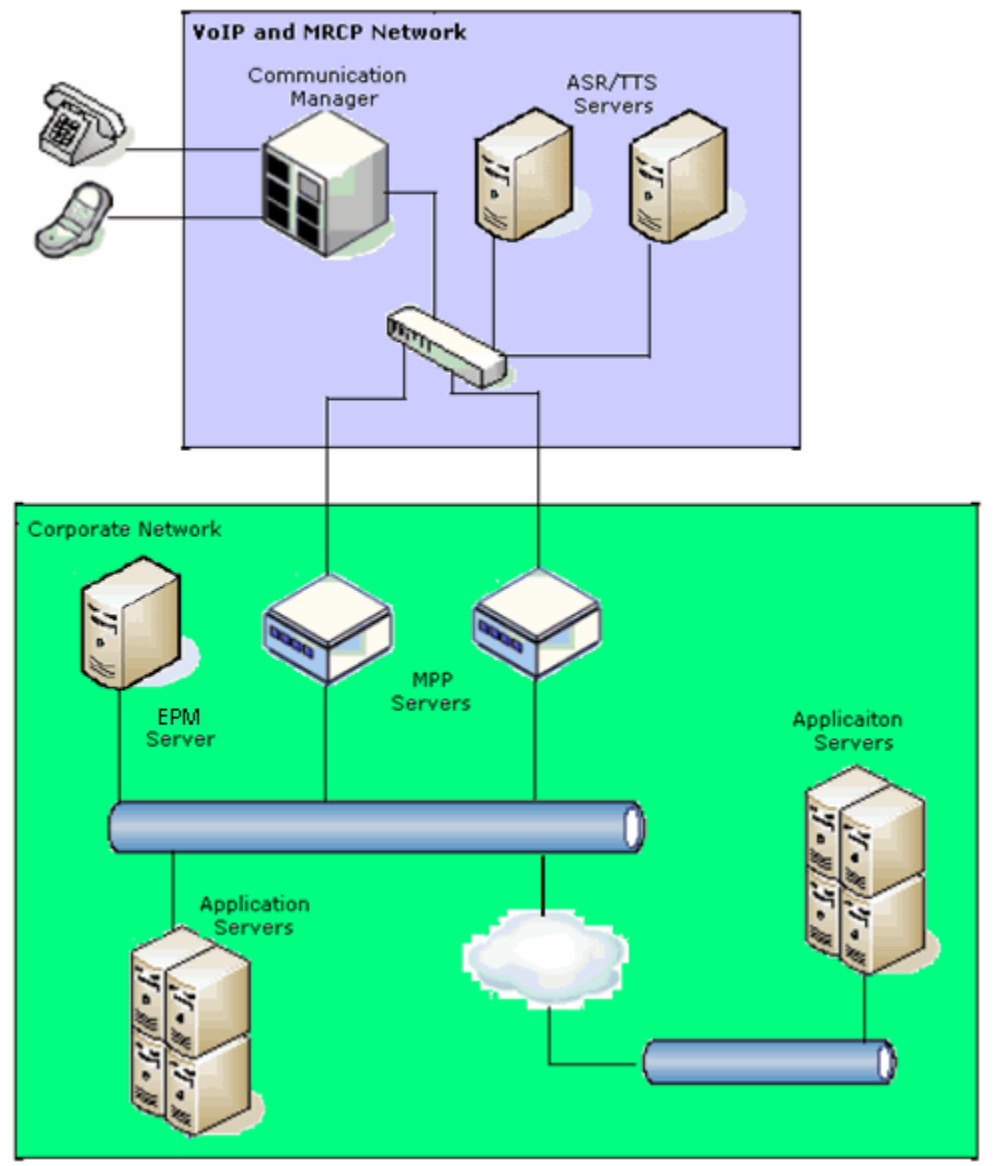
  The corporate network segment carries the network traffic for Media Processing Platform (MPP) system configurations and MPP monitoring. The Experience Portal Manager (EPM) downloads the system configurations to the MPPs and also monitors the MPPs. This segment also carries the network traffic generated 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 Aura® 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.

Redundancy and high-availability

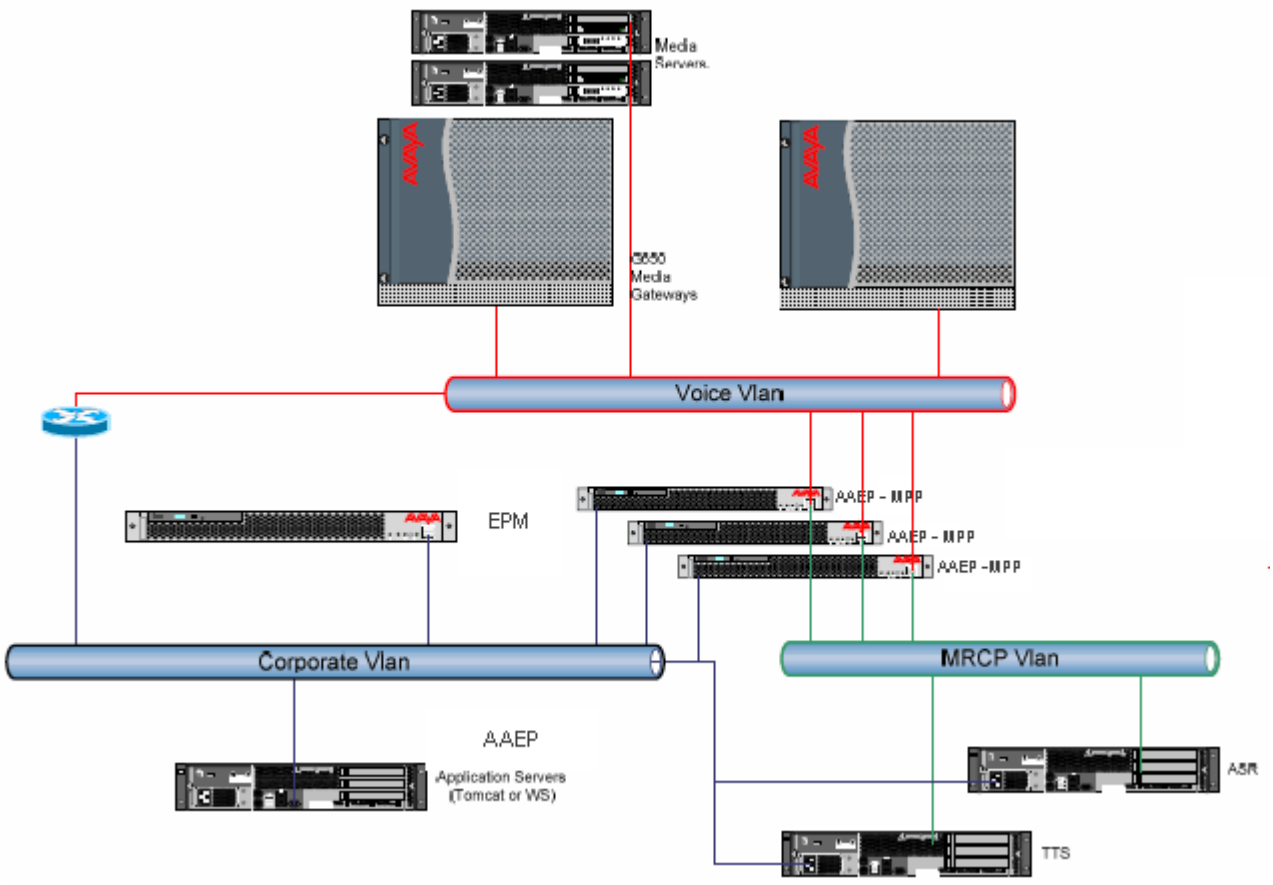
License management

By using Web License Manager (WebLM), you can 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 the licenses to EPM. The WebLM that resides on the EPM is referred to as the Local WebLM. In most small setups of Experience Portal systems, the license is installed on the Local WebLM. In a system that requires redundancy through a WebLM that is installed on a separate server, an Enterprise or Master WebLM is used. Enterprise WebLM allocates licenses to the WebLM that resides on EPM. The location of the 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

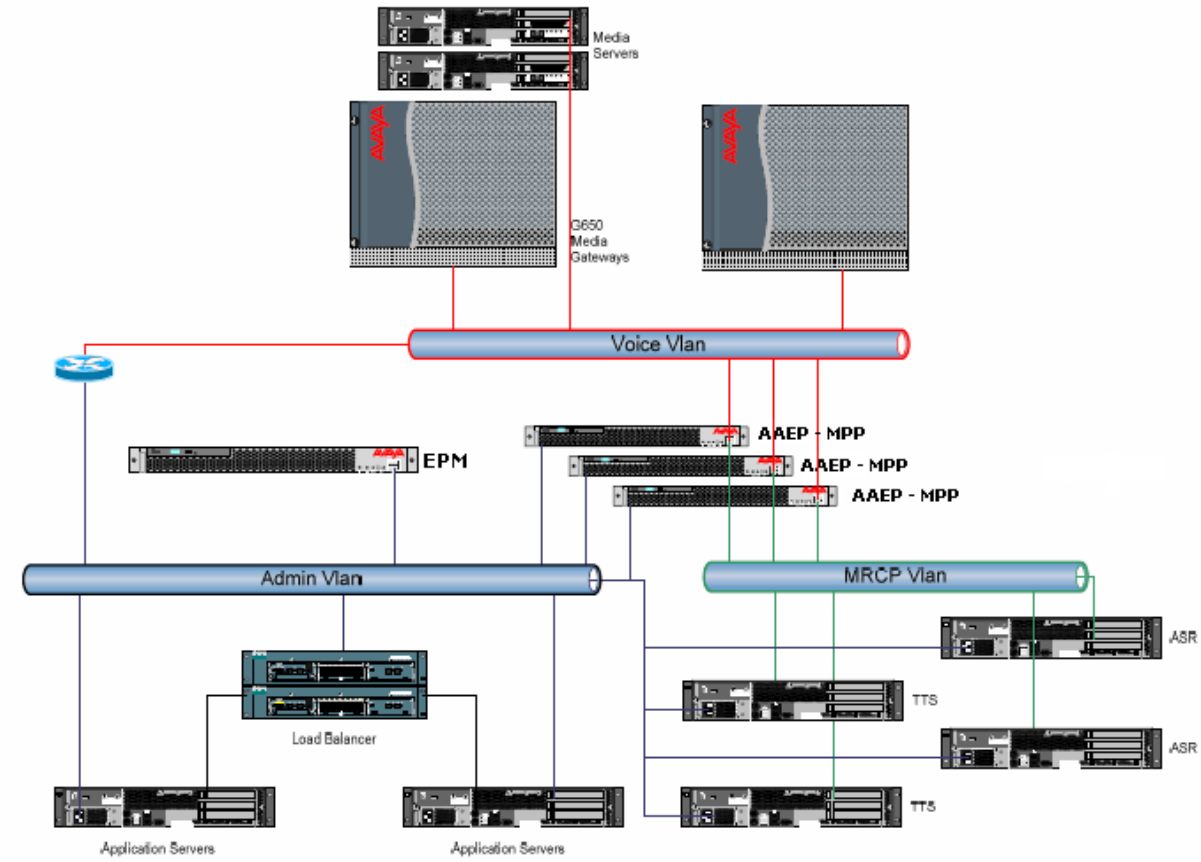
To ensure that the local Experience Portal setup has redundancy for all server components, you have to implement additional hardware while configuring Experience Portal.

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 have to install a high availability 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 there is a hardware failure with any of the server hardware. Local Experience Portal redundancy does not provide redundancy in the event of a network infrastructure failure.



Disaster Recovery site

A very common configuration is to provide a second site with an Avaya Aura® Experience Portal setup which is used when the first site incurs a major system outage. The Disaster Recovery (DR) site mirrors the functionality of the primary site. In many instances, the primary site may be built to have redundant speech and application servers, while the DR site is not built for this purpose. The following figure depicts the DR site with an Experience Portal setup that has redundant speech and application servers. The DR site can be configured in two ways: active-passive and active-active.

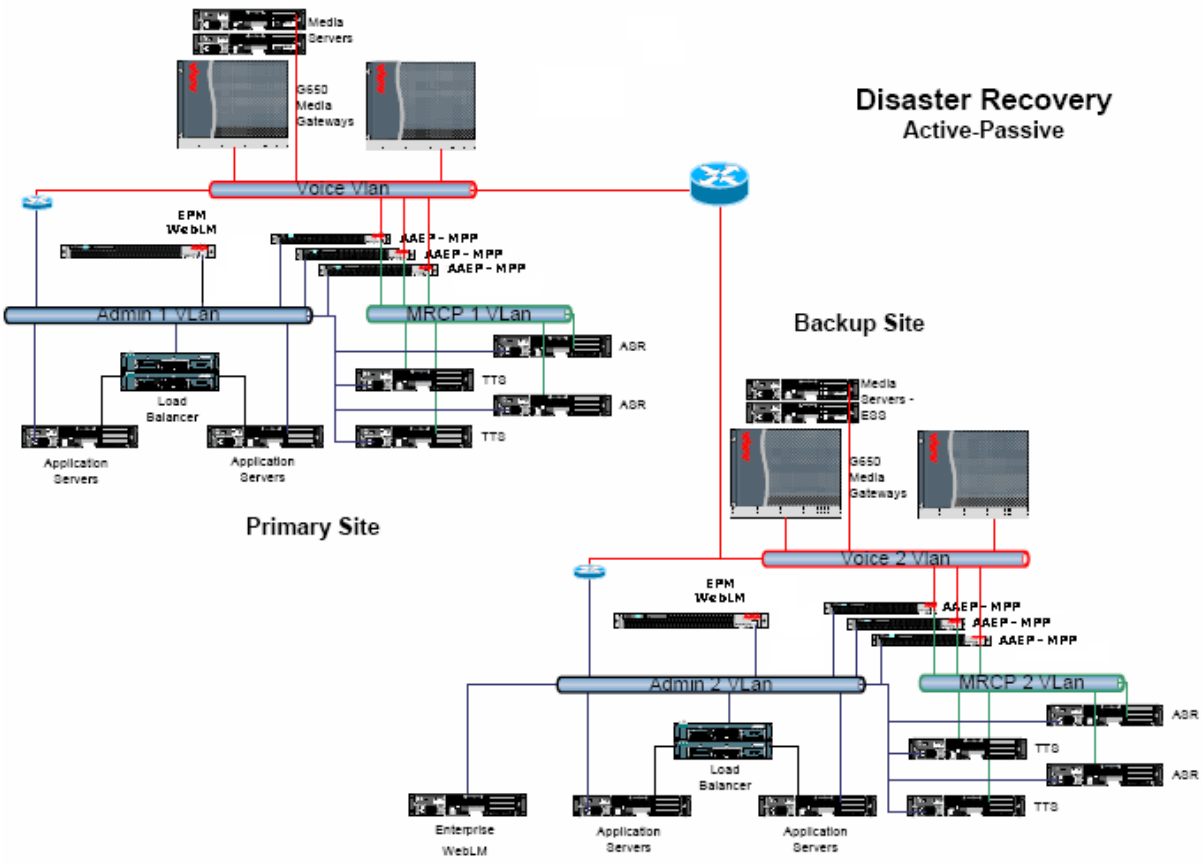


Related topics:

[Active-Passive multi-site configuration](#) on page 43
[Active-Active multi-site configuration](#) on page 44

Active-Passive multi-site configuration

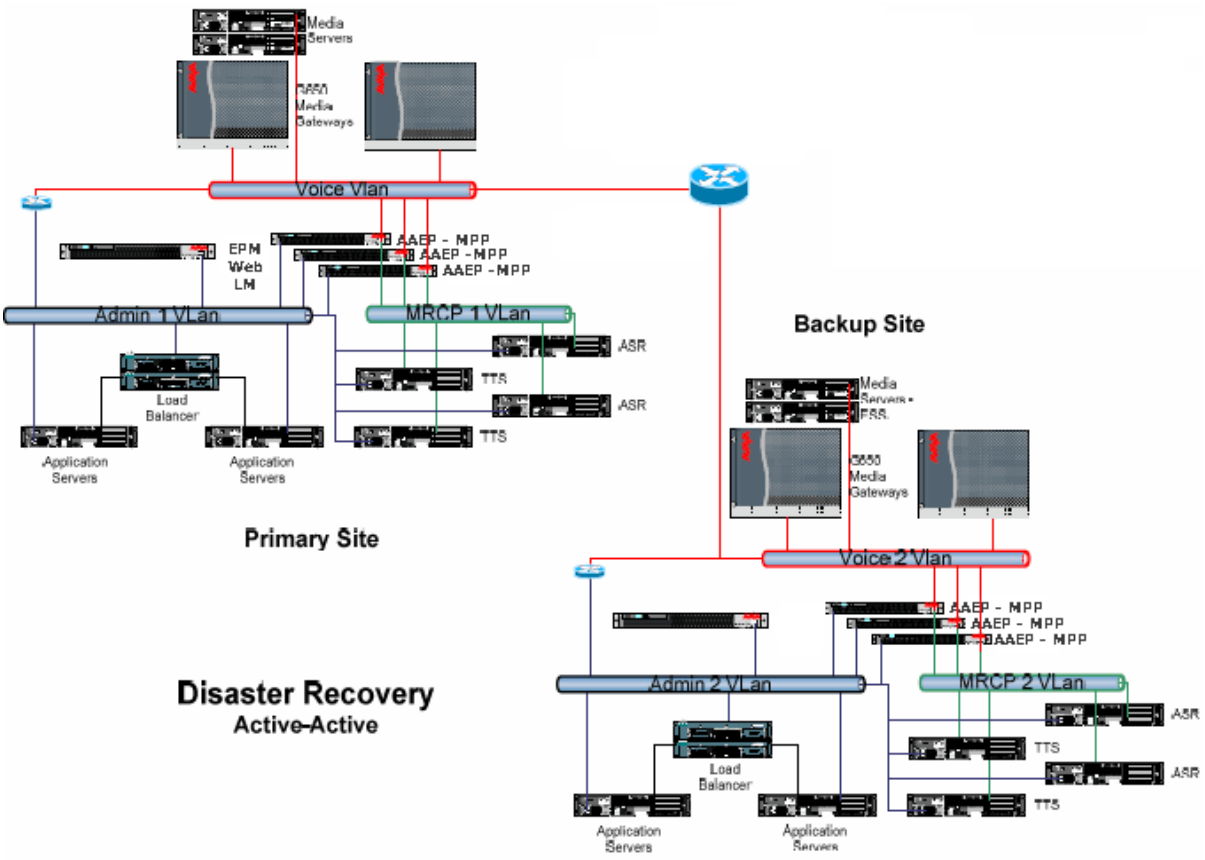
In the active-passive scenario, the DR site is typically not in service and the licenses are shared with the production site. In order to be able to share the Experience Portal licenses between sites, an Enterprise WebLM server must be installed. The following figure depicts a setup that is fully redundant on both the sites with the Enterprise WebLM installed on the backup site. The Experience Portal licenses are installed on the Enterprise WebLM and assigned to the primary site. During a failover, a manual process is implemented to roll the licenses to the backup site. If the Enterprise WebLM server is offline for an extended period, the Experience Portal licenses are valid for 30 days, and are renewed every seven days. If you use the active-passive model, it is critical to test the DR site on a regular interval to ensure that it is kept up-to-date and operational.



Active-Active multi-site configuration

Many global enterprises require the ability to handle all their traffic and functionality at other sites automatically even after they lose a site. They often do this in what is called an active-active configuration where each site is handles a portion of the traffic, but is sized to handle 100% of the traffic if a site is not available for any reason. The primary difference between active-active and active-passive is the Experience Portal licensing. To implement Active-Active DR, Experience Portal licenses must be purchased.

This allows each site to be licensed and active at the same time. Active-active does not require the use of an Enterprise WebLM server if the customer purchases a separate DR license. Each EPM is licensed and configured for full capacity, but only operates at half capacity during normal operations. If one site fails, the remaining sites must be able to handle the additional load without human intervention.



Media Processing Platform

If an MPP fails, Experience Portal Manager detects the failure and 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.

Ports are not redistributed across zones.

Speech servers

Speech servers support a load balancing mechanism across the servers. If a single server fails, the recognition requests and TTS requests go to a backup server. Disaster recovery licensing supports the additional capacity.

The MPP determines which ASR/TTS server to use by looking at Speech server state and languages required by the application Speech server status such as errors and latencies.

The Nuance Speech offer and Loquendo Speech offer uses Disaster Recovery Sales Material Codes.

Speech servers in a zone are only load balanced across MPPs within the same zone.

Application servers

Experience Portal load balances by using the two VXML URLs that are configured with the applications and assigns both URLs to the Voice XML Interpreter (VXI), in any order, to fetch the application VXML. The VXI uses the first URL to fetch the VoiceXML application. However, if the first URL fails, the VXI use s the second URL. When the second URL fails, the VXI reports a failure.

Each MPP polls, every 30 seconds, the application servers that host the VXML applications. If the application server fails to respond to the poll, the server is marked as unavailable. The URL that is referenced by the application server is not used until service is restored and the server responds to the poll. Depending on system load and the time during which the application server fails between polls, it might take time, such as one minute, for the system to mark the application server as offline and stop routing traffic to the unavailable application server.

The load balancing setting of the order of the URLs is arbitrary to provide even loading across multiple application servers during heavier call volumes. Customers that have larger solutions might require a commercial or third-party load balancing solution. For example, customers with high sensitivity for server failure detection or systems where three or more application servers are used, require a load balancing solution. Experience Portal can work with load balancers, such as F5 Big IP and EQulibrium, without any special configurations on Experience Portal.

Multiple application servers provide for capacity and redundancy. Standard web load balancing techniques provide load balancing and failover.

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.

VOX Specific

Configure the IC Connector to implement failover so that the VOX server initiates the connection to the IC Connector. On the IC server, multiple VOX servers are set up so in case one VOX server stops operating, another server starts up. When the IC Connector starts up, the Connector serves calls only when the VOX server initiates a connection.

VRUSM Specific

VRUSM supports automatic failover. If you configure multiple VRUSM servers, then Interaction Center Connector (ICC) communicates with the servers by sending each command to a different VRUSM in the list. If any VRUSM fails either by detection of a failed ping response, or if ICC cannot communicate with the VRUSM server on a prior request, ICC removes the VRUSM server from the active server list. The ICC then pings the VRUSM server on a periodic basis to determine if the server is active. If the server becomes active, ICC includes the server back in the list of active servers for further commands.

Manual changes

PSTN carrier for the failed location must redirect calls to the working location.

System recovery

As with any other application running on a server, being prepared to do a partial or complete Experience Portal system restoration if a disaster occurs is important.

Experience Portal systems should be backed up regularly. 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 should also document the components and settings for the Experience Portal system to facilitate the efforts required to restore the systems. These system records should 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 (HP ProLiant DL360 G7)

Base Unit	Baseline	Options
DL 360 G7	1 U Chassis, Dual Socket	Avaya does not support additional options.
Processor	Intel E 5620 Quad Core/2.4 GHz (Westmere) 3 memory channels per CPU with up to 3 RDIMMs per channel. **Note:** Most applications use 1 or 2 RDIMMs per channel to optimize memory speed.	Intel X5670 six Core/ 2.93 GHz (Westmere) Upgradable to dual processors for either E5620 or X5670.
Memory	12-GB DDR3 RDIMMs (1333 MHz)	N/A
HW RAID 1	P410i RAID controller with 256-MB cache and battery backup. Optioned as RAID 1 or 5.	N/A
Hot-Plug disk drive cage	4 Small Form Factor 2.5" hot-plug hard drive bays are available when an optical device is installed.	HP offers servers with 8 drive bays that do not support an optical drive (not supported by Avaya).
Disk Drive	146-GB 2.5" 10k RPM 6G DP Hard Drive. Two base configurations: 136 total: RAID 1,2 x 146-GB drives 272 total: RAID 5,3 x 146-GB drives	Additional 10-GB 10K RPM drive (4 maximum with optical drive). High performance 146-GB 15k drives 300-GB 100K HDD

Base Unit	Baseline	Options
NICs	4 integrated ENET Gigabit NIC ports with TCP offload engine included on motherboard.	HPNC382T PCI Express Dual Port Gigabit NIC expansion card (Broadcom 5709 silicon)
PCI slots	2 PCI-Express Gen 3 Expansion slots: 1). full-length,full-height slot 2). low-profile slot (1-FL/FH x 16 PCIe and 1-LP x 8 PCIe Riser)	Meeting Exchange Recording uses a PCI-X riser in place of the low-profile PCIe riser in the standard server.
Removable media	Slim line SATA DVD-RW optical drive (used in all Avaya configurations).	Avaya does not support additional options.
Power supply	460 W hotplug AC power supply	750 W AC power supply 1200 W DC power supply Single and dual power supply configurations
Fans	3 fan modules (fan redundancy standards)	Avaya does not support additional options.
Additional items	1 front USB, 2 back USB,1 internal USB	

Environmental specifications

Specification	Value
Temperature range	**Note:** 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. No direct sunlight allowed.
Operating	10°C to 35°C (50°F to 95°F)
Shipping	-40°C to 70°C (-40°F to 158°F)
Maximum wet bulb temperature	28°C (82.4°F)
Relative humidity	**Note:** Storage maximum humidity of 95% is based on a maximum temperature of 45°

Specification	Value
	C (113°F). Altitude maximum for storage corresponds to a pressure minimum of 70 kPa.
Operating	10% to 90%
Non-operating	5% to 95%

Physical specifications

Specification	Value
Dimensions	Height: 4.32 cm (1.70 in) Width: 42.62 cm (16.78 in) Depth: 69.53 cm (27.38 in)
Weight (maximum 2 processors, 2 power supplies, 8 hard disk drives)	15.97 kg (35.20 lb)
Weight (minimum 1 processor, 1 power supply, no hard drives)	14.51 kg (32.00 lb)
Weight (no drives installed)	14.06 kg (31.00 lb)

Related topics:

LAN requirements on page 35
Site requirements on page 36

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. Any additional software that is installed on the system must be installed under a policy of permissive use. Avaya cannot ensure that such software does not affect the operation or performance capabilities of the Avaya Aura® 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 in order 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 to Avaya by sending 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 Web site, http://support.avaya.com/security.

Whether or not immediate support is required, report all toll fraud incidents perpetrated on Avaya services to Avaya Corporate Security to securityalerts@avaya.com. In addition, for information concerning secure configuration of equipment and mitigation of toll fraud threats, see the *Avaya Toll Fraud and Security Handbook* at http://support.avaya.com/css/P8/documents/100073832 .

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.

Related topics:

Secure system access on page 55
Antivirus software on page 56
Network services on page 57
Linux hardening on page 58

SNMP agents and traps on page 59
Secure Sockets Layer on page 60
Avaya Secure Access Link (SAL) and Access Security Gateway (ASG) on page 60

Secure system access

One 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

Network services are subject to security vulnerabilities which unfortunately allow unauthorized users to gain access to the system. The Experience Portal system uses relatively few network services, and several unneeded services and ports are disabled during the installation of Avaya Enterprise Linux as part of the bundled server offer.

The network services that are enabled during Avaya Enterprise Linux and Experience Portal installation are:

- Secure Shell (SSH) (server-side), which runs on all Experience Portal servers.
- Apache Tomcat, which runs on the EPM server. Tomcat is a J2EE compliant servlet container and is the default application server for the EPM.
- Network Time Protocol (NTP), which runs on all Experience Portal servers.
- PostgreSQL (SQL server), which runs on the EPM server. Postgres is an SQL compliant, open source, object-relational database management system for the Experience Portal database.
- Apache HTTPD, which runs on the MPP servers. The MPP servers use the Apache Web Server to implement web services for EPM monitoring and control and the Media Server Service Menu.

For more information about how Experience Portal protects sensitive data, see the Avaya Aura® Experience Portal 7.0 Security White Paper in the Print guides section of the Avaya Aura® Experience Portal Documentation Library.

Related topics:

Secure Shell on page 57
Network Time Protocol on page 58

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.

In order to do so, the Experience Portal software installer changes the `ntp.conf` file on each server on which the software is installed. When you install the:

- Primary EPM software, the `ntp.conf` file on that server is set to point to the local clock.
- MPP software or the auxiliary EPM software, the `ntp.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 Aura® 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, along with information about the target objects that the SNMP agent can interact with using these commands and queries, is stored in a Management Information Base (MIB) that resides on the managed device.

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.

Secure Sockets Layer

Experience Portal provides SSL support for the following:

- EPM administration traffic runs over an SSL/HTTPS connection. Using an SSL/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 SSL/HTTPS.
- You can configure the Avaya Voice Browser to use SSL 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 SSL for VoiceXML, you must install an SSL certificate for each web server domain referenced by an application to fully implement client authentication using SSL for VoiceXML.

Avaya Secure Access Link (SAL) and Access Security Gateway (ASG)

Dial-in lines on the Experience Portal system can be protected by an Avaya-developed solution called Access Security Gateway (ASG). The ASG package is integrated into the Experience Portal system and provides secure authentication and auditing for all remote access into the maintenance ports.

ASG authentication is based on a challenge/response algorithm using a token-based private key-pair cryptographic authentication scheme. Secure auditing is also provided. Logs are available that include information such as successful logins, failed logins, errors, and exceptions.

Port utilization

For complete port matrix information, see the Avaya Aura® 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.

Nonsecure data transport

Certain Avaya and third-party products with which Experience Portal interacts do not support secure data transport. Since these remote systems do not yet support this capability, there is not a secure communication link between the following:

- IC connector in a Orchestration Designer application and the Avaya Interaction Center.
- Computer Telephony Integration (CTI) connector in a Orchestration Designer application and the Avaya Computer Telephony (CT) telephony server.
- MPP and the TTS and ASR speech servers.
- Orchestration Designer application reporting and the EPM.

Note:

If this data needs to be secure, a private LAN card can be used to isolate the data from other Experience Portal traffic.

Chapter 7: License requirements

A license file is required for Avaya Aura® Experience Portal operation as it defines the telephony ports and the ASR and TTS connections that you are authorized to use. The Avaya Aura® Experience Portal license file is distributed separately in an email from Avaya.

By using Web License Manager (WebLM), you can 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 the licenses to EPM. The WebLM that resides on the EPM is referred to as the Local WebLM. In most small setups of Experience Portal systems, the license is installed on the Local WebLM. In a system that requires redundancy through a WebLM that is installed on a separate server, an Enterprise or Master WebLM is used. Enterprise WebLM allocates licenses to the WebLM that resides on EPM. The location of the 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 version 4.4 or later, and a valid Avaya Aura® Experience Portal Release 7.0 license must be installed on the license server.

After the EPM receives current information about authorized licenses, it allocates the available licenses among the Media Processing Platform (MPP) servers in the system.

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

Glossary

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.
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.
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.
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	A SIP routing and integration tool 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.
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.
TCP	Transmission Control Protocol is one of the core protocols of Internet Protocol Suite, the set of network protocols used for the Internet.
TLS	Transport Layer Security (TLS) is a cryptographic protocol that provide communication security over the Internet.

Index

M

N

O

P

R

S

T

V

W

Z