Avaya Experience Portal 8.1.2.3 Security White Paper

Issue 1.0
August 2025

Abstract

This paper provides information about the security strategy for Avaya Experience Portal 8.1.2.3 and provides suggestions that companies can use to improve the security of their Avaya Experience Portal systems and applications.

Contents

1. Overview

The Avaya Experience Portal system relies on many interconnected hardware and software components to process the deployed applications. This paper details each component, interactions, default security configurations, and suggests improvements, such that the overall system security can be tailored per installation. As appropriate for the target environment and needs of deployed applications, consideration for the sensitivity of data utilized by the Experience Portal system should guide decisions concerning security policies for the system. This document discusses how the Experience Portal system uses and protects sensitive data to allow administrators choices in defending their data.

2. Physical Security

All the security measures described throughout this paper assume that physical access to the hardware on which the Experience Portal system runs is strictly controlled. Unrestricted access to the hardware can be exploited, allowing attackers to gain full administrative privileges and override any security settings. As a result, the value of any further steps to secure the Experience Portal system depends on placing the hardware in an isolated and secure location. A minimum number of administrative personnel should be allowed entry to this location to reduce the threat of disturbance, either malicious or accidental, to the Experience Portal system.

3. Network Services and Logical Connections

To prevent the abuse of any security vulnerabilities (future or otherwise) exposed by susceptible network services, only the minimum number of network services required for operation should be enabled. Avaya recommends that customers should not activate additional network services unless a clear business need dictates otherwise. Enabling extraneous network services increases the risk of remote access to the Experience Portal system by unauthorized individuals.

For Experience Portal installations, in which the Avaya Enterprise Linux Installer is used, only required network services will be installed and enabled.

For Experience Portal installations using Red Hat Enterprise Linux obtained from another vendor, ensure that only the required network services are installed and enabled.
Figure 1 shows the network services, ports, and connections needed by the Experience Portal system on Linux

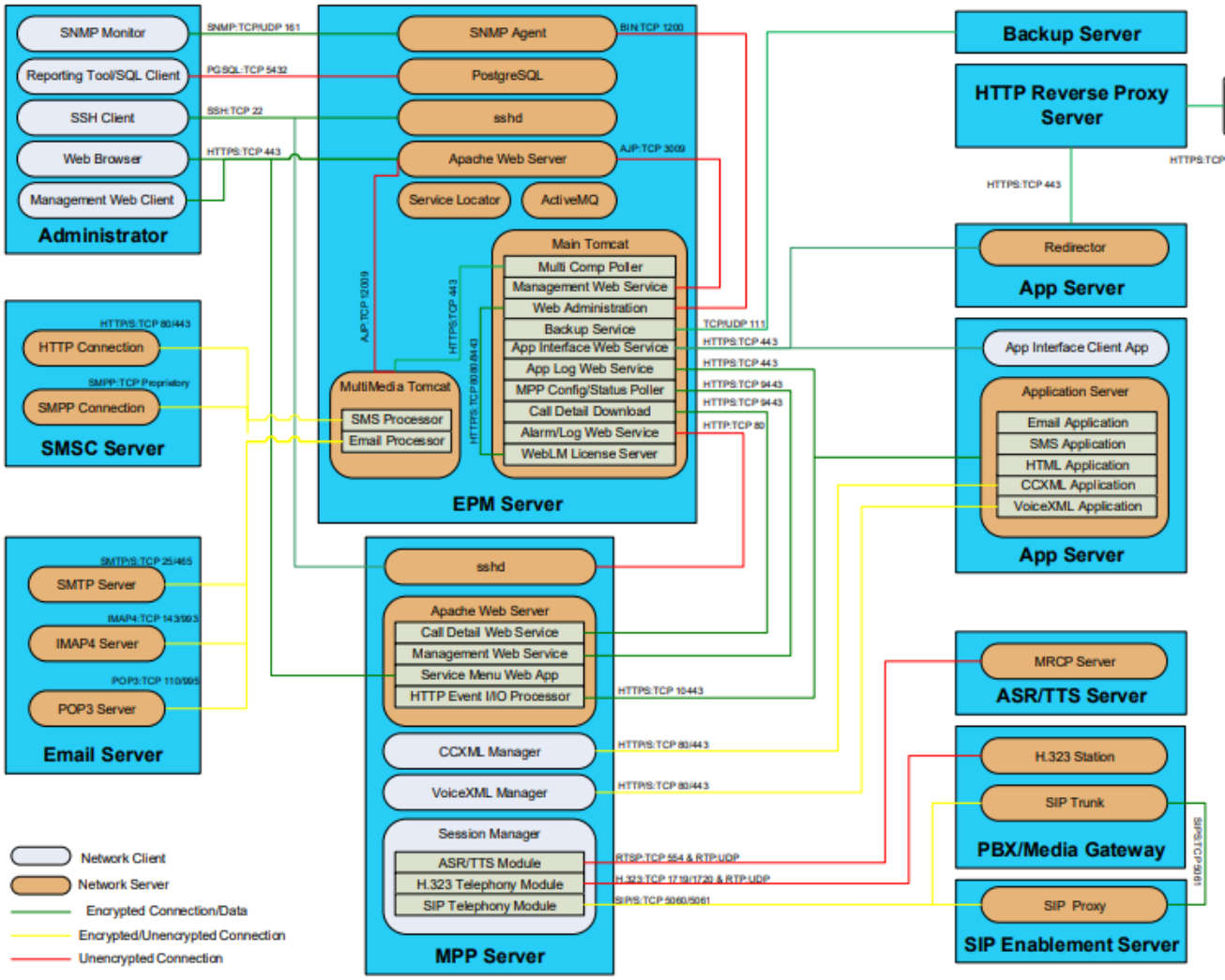

Figure 1: Network services & clients required for operation of the Experience Porta

3.1 Network Services

The following sections describe the network services installed and configured on the Experience Portal Manager (EPM) and Media Processing Platforms (MPPs). Any network services running on these systems that are not listed below are not required for operation and should be disabled.

3.1.1. Secure Shell

Secure Shell (SSH) is a program that includes capabilities for logging into another computer over a network, executing commands on a remote machine, and moving files from one machine to another. Secure Shell provides strong authentication and secure communication over distrusted networks.

Process	Default Port	Protocol	Purpose
sshd	22	TCP	Remote console access and file operations

The SSH server is configured on the EPM and each MPP to utilize TCP port 22 by default. Network traffic from the SSH client on the systems used to administer Experience Portal should be allowed to pass to the EPM and MPP servers to allow remote access and file operations to all the systems.

The options governing the SSH server are set through the **/etc/ssh/sshd_config** file. The default configuration for the SSH server is to use password authentication, employing the accounts provided by the Linux operating system. However, the Experience Portal installation modifies the SSH configuration so that users in the root group are unable to log in remotely. This enforces the requirement that remote logins escalate to get root privileges, buffering unrestricted remote console access of the system. This is accomplished by adding the following line to the **sshd_config** file:

DenyGroups root

If a **DenyGroups** line is already specified in the file and does not contain the root group in the list of restricted groups, then the line is not modified and a warning message is displayed.

To enhance the security of the SSH server, the **Protocol** option in the **sshd_config** file is set to only allow SSH2 connections

Protocol 2

As SSH1 protocol is subject to several vulnerabilities, it is highly recommended that this option is not modified to allow SSH1 clients to connect to the Experience Portal system. Also, the SSH weak algorithms have been removed which make break older SSH clients. It is recommended that SSH clients which support strong algorithms are used for connecting to the servers.

One additional modification can be optionally made to further enhance the security of the SSH server, depending upon the operating environment for the Experience Portal system. Public key authentication can be used instead of password authentication, and password authentication can be disabled. Setting up this configuration requires the creation and management of key files that are beyond the scope of this paper, but public key authentication allows strict control over which logins can be accessed remotely and which personnel are authorized to use those logins.

Key Exchange (KEX) / Message Authentication Code (MAC) / Cipher Algorithms

In 8.1.2 the following Ciphers , MAC and KEX algorithms are set. Testing has been executed on the current settings and any changes to them while possible should be tested prior to going to production. The sshd_conf file controls what is set/used.

Type	Default settings
Ciphers	aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com
MACs	hmac-sha2-256,hmac-sha2-512,umac-128@openssh.com,hmac-sha2-256- etm@openssh.com,hmac-sha2-512-etm@openssh.com,umac-128- etm@openssh.com
KEX	diffie-hellman-group-exchange-sha256,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521

3.1.2. Apache Tomcat Service

The Apache Tomcat service is a Java servlet container that is used to implement and consume most of the Web services required for the operation of the EPM server. Most visible is the Web Administration utility used to configure and manage the entire Experience Portal system. In addition, several Web services are accessible to allow MPPs and Application Environments (AE) to log events and alarms to the EPM and to allow the initiation of outbound calls.

Process	Default Port	Protocol	Purpose
java	3005	tcp	Tomcat shutdown command
java	3009	tcp	Tomcat AJP connection handler
java	31050	tcp	Avaya Operation, Administration and Maintenance (OAM) handler
java	50200	tcp	Avaya Operation, Administration and Maintenance (OAM) handler

Apache Tomcat runs only on the EPM and uses two TCP ports. TCP port 3005 is used to send shutdown command to the Tomcat process. This port is bound to the loopback address only and is not accessed outside the EPM. TCP port 3009 is used for Apache JServ Protocol (AJP) connections to the Tomcat process. This port is also bound to the loopback address and is not accessed from remote clients. Starting with version 4.0, connections to the services exposed by Apache Tomcat are made through the Apache HTTP server. The HTTP server then utilizes AJP connections to Tomcat to complete the requests. No direct TCP connections to Tomcat are needed.

TCP ports 31050 and 50200 are used by the Web Administration to synchronize configuration changes. Remote access to these ports isn't required.

3.1.3. Apache Tomcat Multimedia Service

The Apache Tomcat Multi-Media service is a Java servlet container that is used to implement the multi-media features supported by the EPM server. This service was added in version 7.0 and is responsible for processing inbound and outbound multi-media messages.

Process	Default Port	Protocol	Purpose
java	12005	tcp	Tomcat shutdown command
java	12009	tcp	Tomcat AJP connection handler

This service runs only on the EPM and uses two TCP ports. TCP port 12005 is

used to send shutdown command to the Tomcat process. This port is bound to the loopback address only and is not accessed outside the EPM. TCP port 12009 is used for Apache JServ Protocol (AJP) connections to the Tomcat process. This port is also bound to the loopback address and is not accessed from remote clients. Connections to the services exposed by Apache Tomcat are made through the Apache HTTP server. The HTTP server then utilizes AJP connections to Tomcat to complete the requests. No direct TCP connections to Tomcat are needed.

3.1.4. Apache Tomcat Application Service

The Apache Tomcat Application service is a Java servlet container that can be used to host the Orchestration Designer applications

Process	Default Port	Protocol	Purpose
java	7005	tcp	Tomcat shutdown command
java	7009	tcp	Tomcat AJP connection handler
java	7080	tcp	Tomcat HTTP connection
java	7443	tcp	Tomcat HTTPS connection

This service can only be installed only on the EPM. TCP port 7005 is used to send shutdown command to the Tomcat process. This port is bound to the loopback address only and is not accessed outside the EPM. TCP port 7009 is used for Apache JServ Protocol (AJP) connections to the Tomcat process. This port is also bound to the loopback address and is not accessed from remote clients.

TCP port 7080 is for handling HTTP requests from remote clients and TCP port 7443 is for handling HTTPS requests from remote clients. By default TCP port 7443 is not enabled and the Tomcat configuration needs to be updated to enable this port.

Note:
This service does not get installed automatically and needs to be installed manually in case there is a need to host either the Redirector application or Orchestration Designer applications on an application server which is co-resident with the EPM

3.1.5. Apache Tomcat WebLM Server

New to 8.1.2 an additional Apache Tomcat instance has been added to facilitate the co-resident WebLM Server features supported by the EPM server.

Process	Default Port	Protocol	Purpose
java	4005	tcp	Tomcat shutdown command
java	4009	tcp	Tomcat AJP connection handler

This service runs only on the EPM and uses two TCP ports. TCP port 4005 is used to send shutdown command to the Tomcat process. This port is bound to the loopback address only and is not accessed outside the EPM. TCP port 4009 is used for Apache JServ Protocol (AJP) connections to the Tomcat process. This port is also bound to the loopback address and is not accessed from remote clients. Connections to the services exposed by Apache Tomcat are made through the Apache HTTP server. The HTTP server then utilizes AJP connections to Tomcat to complete the requests. No direct TCP connections to Tomcat are needed.

Note
In previous releases, WebLM web requests to Apache httpd were forwarded to AJP port 3009 – which was the AJP port for the main EPM Tomcat instance.

From 8.1.2 this is not now the case and the ports mentioned above (4005/4009) are the ports being used.

The Apache httpd configuration has changed whereby web requests targeted at secure port 8443 (WebLM) now go to AJP port 4009 which forwards the web requests into the WebLM Server Tomcat.

3.1.6. Apache HTTP Server

The Apache HTTP Server is an open-source HTTP server employed by both the EPM and MPPs. The EPM uses the HTTP server to front-end requests to the Apache Tomcat server. The MPPs utilize the HTTP server to implement various Web services and the service menu. The EPM uses the Web services to control and monitor individual MPPs. The service menu provides access to troubleshooting tools to diagnose a particular MPP.

Process	Default Port	Protocol	Purpose
httpd	80	tcp	Apache Web Server HTTP connection handler
httpd	443	tcp	Apache Web Server HTTPS connection handler for SSL requests
httpd	8080	tcp	HTTP connection handler. Forwards to Apache Tomcat for WebLM access
httpd	8443	tcp	HTTPS connection handler. Forwards to Apache Tomcat for secure WebLM access. (See section 3.1.5)
httpd	9443	tcp	Apache Web Server HTTPS connection handler for SSL requests for Web Services.
httpd	10443	tcp	Apache Web Server HTTPS connection handler for SSL requests for “basic http i/o” events.
httpd	11443	tcp	Apache Web Server HTTPS connection handler for SSL requests for synchronizing trusted certificates between the EPMs.

The number of ports opened by the Apache HTTP network service varies for the EPM, MPP, or single box system. TCP ports 80 and 443 are always configured to be open. TCP port 80 is the HTTP connection handler and is not directly used by the Experience Portal system. Any requests to the Web services or applications through this connection handler will simply be redirected to the secure HTTPS connector (port 443), forcing the use of HTTPS and Transport Layer Security (TLS) for all data transfers. The secure HTTPS connection handler on TCP port 443 is the primary interface to the applications and services on the EPM or MPP.

Note:
TCP Port 80 is required however when the default certificate configuration is in place and when the first connection from the EPM to the MPP/Aux EPM is initiated. This is when the default root signing certificate trusted certificate is passed automatically to any other EPM server to facilitate secure TLS communications.

The certificate passed is a public trusted certificate which allows EPM to complete a TLS handshake with MPP/Aux EPM.

In addition to these two standard ports, the EPM is also configured to open TCP ports 8080 and 8443). These ports are configured to only allow access to the Avaya WebLM licensing server. TCP port 8080 allows legacy applications to access WebLM using an unsecured connection. TCP port 8443 allows for a secure connection, using TLS.
See Section 3.1.5 on new Apache Tomcat instance for WebLM server for AEP 8.1.2.

TCP port 9443 is configured on the MPP to allow the EPM access to the necessary Web services for management and configuration of the MPP. This connection handler is setup to enforce a secure connection, using TLS, and is protected with certificates requiring the EPM and MPP to mutually authenticate. Further details on the use of TLS and certificates are provided in Section 5.

TCP port 10443 is configured on the MPP to allow transport of events between the CCXML HTTP Event I/O processor in the MPP and the external components for active CCXML sessions.

TCP port 11443 is configured on the Primary EPM to allow synchronizing of the trusted certificates on the Auxiliary EPM from the Primary EPM.

For a single box system, all of these TCP ports are configured to be open.

As a part of AEP 8.1.2.3 , HSTS response header is configured on the webserver to instruct the browser to only communicate via HTTPS inorder to avoid downgrade attacks, SSL-Stripping man-in-middle attacks and weakening of the cookie hijiacking protections.

3.1.7. Chrony

NTP was the primary time keeping service used in previous releases of AEP. In8.1 we have migrated to use chrony. Since AEP 8.0 supports RHEL 7 and 8 and in Red Hat Enterprise Linux 8 ,ntp is no longer supported. chrony is enabled by default and as such to have common installation chrony is used in both RHEL 7 and 8 offerings. A script is executed to move to chrony and as such the files used are changed. See table below

ntp name	chrony name
/etc/ntp.conf	/etc/chrony.conf
/etc/ntp/keys	/etc/chrony.keys
ntpd	chronyd
ntpq	chronyc
ntpd.service	chronyd.service
ntp-wait.service	chrony-wait.service

3.1.8. PostgreSQL

PostgreSQL is the highly scalable, SQL-compliant, open-source object-relational database management system used by the Experience Portal system to store configuration, logging, and alarm data.

Process	Default Port	Protocol	Purpose
postmaster	5432	tcp	Remote access to the Experience Portal database

To enable the generation of custom reports, network traffic from the reporting tool or PGSQL client on the systems used to administer Experience Portal should be allowed to reach the EPM through TCP port 5432. The PostgreSQL server is configured to run only on the EPM. By default, a database user named “postgres” is created and has read/write access to all the database tables. This user is disabled for remote access.

By default, the PostgreSQL configuration authorizes only a single database user for remote access. During the Experience Portal installation, the password for database users named "report" and “vpcommon” is set and granted access to the few tables related to logging and reporting in the Experience Portal database. Database access is controlled by the settings in the **/var/lib/pgsql/data/pg_hba.conf** file and privileges are assigned by using the GRANT command.

3.1.9. SNMP Agent

The SNMP Agent allows third-party network management software to monitor the status of the Experience Portal system, using the SNMP protocol.

Process	Default Port	Protocol	Purpose
jsvc.exec	161	udp	SNMP server
jsvc.exec	1200	tcp	SNMP Agent control messages

By default, the SNMP Agent, when enabled, will use UDP port 161 and TCP port 1200. UDP port 161 is used to serve the SNMP protocol to remote network management software. The SNMP Agent will not listen on port 161 unless at least one SNMP protocol version is enabled on the SNMP Agent Configuration page in the Experience Portal Web Administration. The port number and transport protocol can also be adjusted from this configuration page if necessary. TCP port 1200 is used by the Experience Portal Web Administration to send control messages to the SNMP Agent. This port is only accessed by the EPM server and need not be exposed for remote traffic.

3.1.10. Apache ActiveMQ

The Apache ActiveMQ service implements a message broker which supports the Java Message Service (JMS) 1.1 API.

Process	Default Port	Protocol	Purpose
java	61616	tcp	JMS message broker default transport connector

The Apache ActiveMQ network service is only configured to run on the EPM. Traffic to both the ports only originates from the EPM. These ports need not be exposed to outside access.

3.1.11. Avaya Service Locator

The Avaya Service Locator service is used to support the logging and alarming Web services used by the Experience Portal System.

Process	Default Port	Protocol	Purpose
java	10000	tcp	Web service locator

The Avaya Service Locator network service is only configured to run on the EPM. Traffic to TCP port 10000 need not be exposed to remote access.

3.2. Network Clients

The following sections describe the network clients installed and configured on the EPM and MPPs. These processes require access to certain network resources and should be allowed to establish the network connections outlined below.

3.2.1. VoiceXML Manager

The VoiceXML (VXML) Manager process performs all tasks necessary to fetch, interpret, and process VoiceXML applications, by requesting resources from the Session Manager process.

Process	Default Port	Protocol	Purpose
vxmlmgr	80	tcp	HTTP transfer of VXML pages
vxmlmgr	443	tcp	Secure HTTPS transfer of VXML pages using SSL

The VXML Manager process makes HTTP and HTTPS client requests to a VXML application server by using TCP ports 80 and 443 by default. Other ports are possible, if specified in the Application URL. Network traffic from the MPPs to the VXML servers on these ports should be permitted.

By default, VXML applications are configured to use regular HTTP requests to transfer VXML pages from the VXML application servers. This setting eliminates the overhead required to encrypt and decrypt the data transferred but is potentially vulnerable to eavesdropping. If the VXML application contains sensitive information, encryption can be enabled by using the HTTPS protocol. The HTTPS protocol transports data by using a secure SSL or TLS connection.

If an application is enabled to use a secure HTTPS connection, it may be necessary to install trusted application certificates, using the Trusted Certificates tab on the Certificates page through the Web Administration. Refer to the product documentation for detailed instructions.

3.2.2. CCXML Manager

The CCXML Manager process performs all tasks necessary to fetch, interpret, and process CCXML applications, by requesting resources from the Session

Manager process.

Process	Default Port	Protocol	Purpose
ccxmlmgr	80	tcp	HTTP transfer of CCXML pages
ccxmlmgr	443	tcp	Secure HTTPS transfer of CCXML pages using SSL
ccxmlmgr	10443	tcp	Secure HTTPS transfer of “basichttp” events

The CCXML Manager process makes HTTP and HTTPS client requests to a CCXML application server by using TCP ports 80 and 443 by default. Other ports are possible, if specified in the Application URL. Network traffic from the MPPs to the CCXML servers on these ports should be permitted.

By default, CCXML applications are configured to use regular HTTP requests to transfer CCXML pages from the CCXML application servers. This setting eliminates the overhead required to encrypt and decrypt the data transferred but is potentially vulnerable to eavesdropping. If the CCXML application contains sensitive information, encryption can be enabled by using the HTTPS protocol. The HTTPS protocol transports data by using a secure SSL or TLS connection.

If an application is enabled to use a secure HTTPS connection, it may be necessary to install trusted application certificates, using the Trusted Certificates tab on the Certificates page through the Web Administration. Refer to the product documentation for detailed instructions.

The CCXML browser is capable of decoding and decrypting CCXML files which have been encrypted using standard Blowfish 128bit encryption and then encoded using base64 encoding. To generate the encrypted and encoded CCXML files, a CCXML encryption tool called ContentEncoder has been developed. The ContentEncoder encrypts a static CCXML page by first running it through a standard Blowfish 128bit encryption and then base64 encode the encrypted content. The encoded content generated by ContentEncoder is supposed to be stored on the application server and fetched by the CCXML browser when the CCXML application is executed. After the CCXML browser fetches a file that has been encoded by ContentEncoder it automatically decodes and decrypts it. The encryption/decryption key is built into both the ContentEncoder and the CCXML browser.

The ContentEncoder tool is only for internal use at Avaya.

3.2.3. Session Manager

The Session Manager process on the MPP manages and controls allocated media resources, including Automated Speech Recognition (ASR), Text-to-Speech (TTS) and telephony connections, providing the media connections the VXML Manager needs.

Process	Default Port	Protocol	Purpose
SessionManager	554	tcp	RTSP connections to MRCP servers for ASR and TTS processing
SessionManager	1720	tcp	H.323 connections to PBXs
SessionManager	5060	tcp	SIP connections to the SIP Enablement Server
SessionManager	5061	tcp	Secure SIP connections to the
SessionManager	30000-30999	udp	RTP sessions between the MPPs and MRCP server and the MPPs and PBXs SIP Enablement Server

The Session Manager process opens several network connections to maintain the various media connections required to run the VXML applications. For sessions requiring speech recognition, the Session Manager must open a Real Time Streaming Protocol (RTSP) connection to a Media Resource Control Protocol (MRCP) server providing ASR resources by using TCP port 554. In addition, a User Datagram Protocol (UDP) connection will be established to pass audio data through the Real-Time Transport Protocol (RTP) from the MPP to the ASR resource on the MRCP server. Similarly, sessions requiring TTS will establish another RTSP and UDP connection to an MRCP server providing TTS resources. To process inbound and outbound telephone calls from the Private Branch Exchange (PBX), an H.323 connection will be created for each H.323 station allocated to a particular MPP. The UDP connections used to pass audio data to and from the PBX through RTP will be created and destroyed during a call, as determined by the call control messages passed over the H.323 connection.

An MPP that is configured to use SIP will have either TCP port 5060 or 5061 open. TCP port 5060 is opened when the TCP protocol is selected for transport when configuring the SIP trunk. If the TLS transport is selected, TCP port 5061 will be used. The TLS transport offers encryption and authentication of the call control messages between the MPP and the SIP Enablement Server (SES). Authentication between the Experience Portal system and the SES is controlled by the use of digital certificates and requires that a signing certificate be configured in the Root Certificate tab of the Certificates Page on the Web Administration. Refer to the product documentation for further details. Similar to H.323, UDP connections will be created and destroyed during a call, as needed for the RTP audio data. Media encryption for these links can be enabled through configuration.

The RTSP and RTP connections between an MPP and an MRCP server are unencrypted and subject to eavesdropping. These connections should be protected by isolating the network traffic between the MPPs and the MRCP servers. By default, connections to the PBX are also unprotected. Media encryption can be optionally enabled to protect the RTP streams between an MPP and a PBX should an application require protection of voice data. Enabling this option increases the workload for an MPP, limiting the number of simultaneous calls that a single MPP can process. The H.323 connection will always be unencrypted, even if media encryption is enabled.

3.3. Security Enhancements

3.3.1. Content Security Policy (CSP) Header Configuration

AEP sets the following CSP header to enhance client-side security:

Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data: https://fonts.googleapis.com https://fonts.gstatic.com;

This policy restricts content loading to trusted sources. Scripts and styles are allowed only from the same origin, with limited use of 'unsafe-inline' and 'unsafe-eval' for compatibility. Images and fonts are restricted to self and specific trusted domains, helping mitigate XSS and injection-based attacks.

3.3.2. X-XSS-Protection Configuration

AEP has disabled the X-XSS-Protection header:

Header set X-XSS-Protection "0"

Modern browsers have deprecated this header due to its limited effectiveness and potential side effects. It is now recommended to disable it ("0") when a robust **Content-Security-Policy (CSP)** is enforced. CSP offers a more reliable and modern approach to preventing XSS and content injection attacks.

4. Network Partitioning

By default, the Experience Portal system uses a minimum number of network services and secure network protocols for data transfer to establish a protected environment. However, an extra layer of defense can be implemented by partitioning the network to limit the exposure of certain components of the Experience Portal system. Figure 2 shows a recommended network topology to enhance system security. Although recommended, this configuration is only an example. Many configurations are supported, and this example topology should be tailored to the needs of an individual installation, based on system size and security requirements.

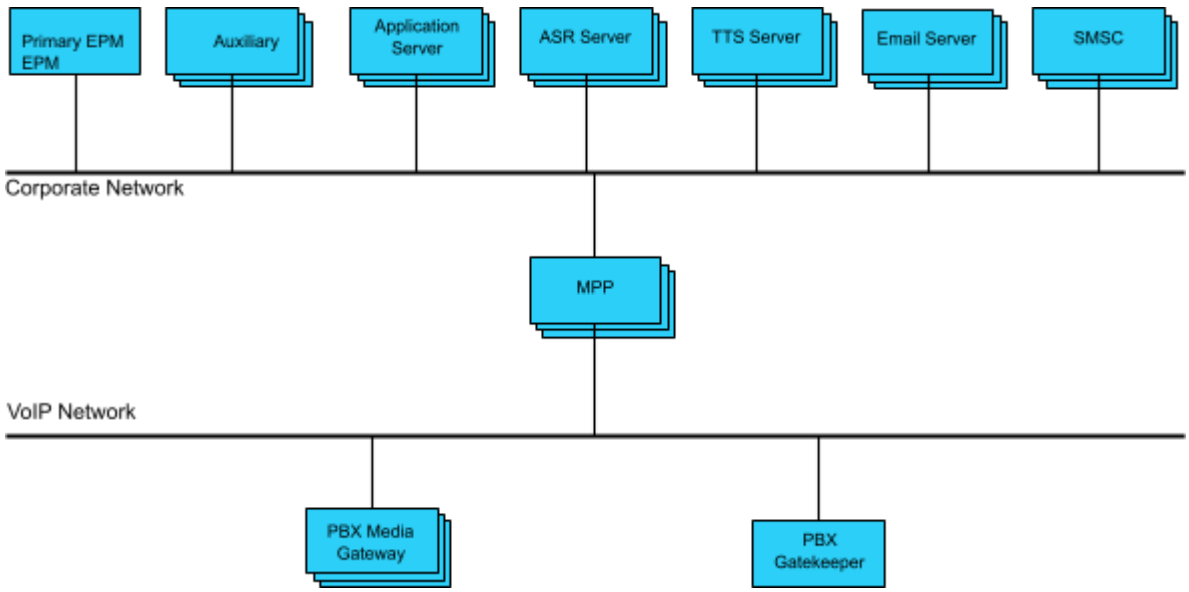

Figure 2: Recommended Network Topology

The recommended network topology has two partitions: the corporate network and the VoIP network. The corporate network segment carries the network traffic for system configuration and maintenance, access to VXML and CCXML applications, and monitoring of the MPPs by the EPM including status polling, logging, and alarming data. This network also transports control and voice data between the MPPs and the ASR/TTS resources provided by the MRCP servers. The VoIP network consists of all of the network traffic between the PBX and the MPPs to establish and process telephony calls.
For a smaller installation, assembling and maintaining all these network segments may not be necessary or desirable. As such, a combination of the network segments is acceptable with consideration for the following security

cautions and assuming that sufficient bandwidth is available to handle expected call volumes. Network requirements are beyond the scope of this paper, but for large systems, partitioning network traffic to simply achieve the total bandwidth required for reliable system operation may be necessary.

The VoIP traffic between MPPs and PBXs can be partially encrypted as an option. The VoIP data for telephony calls consists of two parts: the H.323 call control and the RTP audio data. H.323 call control for telephony calls is never encrypted. Accordingly, call information, such as ANI, DNIS, and chronology, is subject to eavesdropping. If such information is considered sensitive, then the VoIP traffic should be passed through an isolated LAN. Similarly, the RTP audio data for telephony calls is unencrypted by default. If this data cannot be isolated, protection is available through the media encryption option. Enabling this feature consumes extra resources, impacting the maximum number of simultaneous calls on a single MPP, but provides strong protection for any sensitive audio data that may be sent between the MPPs and a PBX.

In order to encrypt the MRCP traffic to and from MPPs, Avaya highly recommends using MRCP v2 protocol with TLS enabled.

Protecting the entire Experience Portal system by using a firewall or other routing limitations on the corporate network segment may be desirable. Using such a system can limit which systems are allowed to establish IP connections with the EPM, MPPs, and other components in the Experience Portal system. A firewall effectively isolates the Experience Portal system from other systems and users that may be sharing the corporate network segment.

5. Transport Layer Security, Ciphers and Certificates

Transport Layer Security (TLS) is a protocol that provides a mechanism for securely transmitting data over the network. The protocol allows client/server applications to use encrypted transmissions and to perform authentication by using digital certificates. This helps prevent eavesdropping, tampering with transmissions, and message forgery.

5.1. TLS

Experience Portal enforces the use of TLS for access to the Web Administration utility, transport of VoiceXML pages, and securing the Web services used by the EPM to monitor the MPPs. Web Administration traffic, including logins and passwords, configuration changes, views of the system configuration, and logs and reports, is required to use a TLS/HTTPS connection. This ensures that no sensitive Web Administration data is transmitted in clear text. The EPM server is authenticated to the Web browser used to access the Web Administration utility

by sending the EPM certificate when the SSL connection is established. If the certificate is self-signed, the browser may present the certificate for acceptance.

The Web services used by the EPM for monitoring the MPPs are also protected by TLS/HTTPS connections. This ensures that any sensitive configuration data or log events are encrypted. Certificates in the TLS connections are mutually authenticated so that the managing EPM, and only this EPM, is ever allowed access to the MPP's Web services.

Application developers can specify whether voiceXML/CCXML/Email/HTML/SMS application data should be transmitted in an encrypted format using SSL/TLS or as clear text. Secure transmission is specified by using a URL that starts with https: when deploying a VoiceXML/CCXML/ Email/HTML/SMS application on the Experience Portal system. If encrypted transmission is not required, the URL can start with http. The server of the VoiceXML/CCXML/ Email/HTML/SMS application is also authenticated by a digital certificate. The VoiceXML/CCXML/ Email/HTML/SMS server certificate sent when negotiating the SSL/TLS connection must be setup as a trusted certificate of type Application on the Trusted Certificates tab on the Certificates page of the Experience Portal Web Administration.

If the SIP connection is configured to use the TLS transport, digital certificates are used to establish a mutually authenticated connection with the SIP Enablement Server. The SIP TLS server certificate sent when negotiating the TLS connection must be setup as a trusted certificate of type SIP Connection on the Trusted Certificate tab on the Certificates page of the Experience Portal Web Administration.

Experience Portal enforces the lowest TLS protocol to be used for secure communications and disables the use of weak protocols by configuring the **SSLProtocol** property in the Apache configuration files for the required secure ports.

Apache Configuration Files	Servers	Ports
/etc/httpd/conf.d/ssl.conf	EPM & MPP servers	443
/etc/httpd/conf.d/vpms.conf	EPM servers	8443 & 11443
/etc/httpd/conf.d/mpp.conf	MPP servers	9443 & 10443

Version	SSL Protocol
8.1.2.3	all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 +TLSv1.2 +TLSv1.3 (Default)
8.1/8.1.1/8.1.2/8.1.2.1/8.1.2.2	all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 (Default)
8.0	all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 (Default)
7.2	all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 (Has to be set)
7.1	all -SSLv2 -SSLv3
7.0.x	all -SSLv2 -SSLv3

This table shows the default lowest TLS protocol accepts by Experience Portal when acting as a TLS Server and when acting as a TLS client.

Version	Acting as TLS Server	Acting as TLS Client
8.1/8.1.1/8.1.2	TLS v1.3	TLS v1.2
8.0	TLS v1.2	TLS v1.2
7.2	TLS v1.2	TLS v1.0
7.1	TLS v1.0	TLS v1.0
7.0.x	TLS v1.0	TLS v1.0

If servers external to Experience Portal servers cannot be updated immediately to use TLS 1.2 or TLS v1.3, then during the transition period, the legacy TLS protocols (TLS 1.0 & TLS 1.1) can be enabled using a command line script that ships with Experience Portal 7.2. The script to enable these legacy TLS protocols is $AVAYA_HOME/Support/Security-Tools/ConfigureLegacyTLS.sh

If the legacy TLS protocols are enabled, it is highly recommended that once the external servers are updated to use TLS 1.2, the script is used to disable the legacy TLS protocols.

Refer to the following topic in the "**Administering Avaya Aura Experience Portal**" document for detailed instructions on enabling/disabling legacy TLS protocols.

- Enabling legacy TLS protocols

External Java based Servers

For any external server which is Java based, including other Avaya products and servers, it is highly recommended that the JDK on the server is upgraded to the latest compatible JDK version that supports TLS 1.2 by default.

5.2 Ciphers

Apart from the protocol to be used for secure connections, Experience Portal also enforces which ciphers will be used for secure communications when acting as a TLS server. It disables the use of weak ciphers by configuring the **SSLCipherSuite property** in the Apache configuration files for the required secure ports

Apache Configuration Files	Servers	Ports
/etc/httpd/conf.d/ssl.conf	EPM & MPP servers	443
/etc/httpd/conf.d/vpms.conf	EPM servers	8443 & 11443
/etc/httpd/conf.d/mpp.conf	MPP servers	9443 & 10443

Version	SSL Cipher Suite
8.1.2.3	FIPS:!3DES:!ADH:!SHA:!EDH:!AES128-SHA256:!AES128-CCM:!AES128-GCM-SHA256:!AES256-SHA256:!AES256-CCM:!AES256-GCM-SHA384 (Default)
8.1.0/8.1.1/8.1.2/8.1.2.2	FIPS:!3DES:!ADH:!SHA:!EDH
8.0	FIPS:!3DES:!ADH:!SHA:!EDH
7.2	FIPS:!3DES:!ADH:!SHA:!EDH
7.1	HIGH:MEDIUM:!ADH:!EDH:!SSLv2:!MD5:!RC4
7.0.x	HIGH:MEDIUM:!ADH:!EDH:!RC4-MD5:!RC4-SHA
6.0.x	HIGH:MEDIUM:!ADH:!EDH

5.3 Certificates

Certificate deployment in Experience Portal is managed using the Primary EPM Administration, this replaces the command line scripts which were the only means in earlier releases. These scripts still exist but it is recommended that customer and administrators use the Primary EPM user interface.

5.3.1.Removal of support for 1024-bit x509 Certificates

In AEP 8.1.2 the crypto level setting on RHEL OS has been set to DEFAULT level which is the recommended level to secure the platform.

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/using-the-system-wide-cryptographic-policies_security-hardening

At this DEFAULT level 1024-bit x509 security certificates can no longer be supported and should be removed and replaced with industry recommended 2048-bit x509 security certificates prior to upgrading to AEP 8.1.2.

5.3.1.1 Upgrade prerequisites when 1024 x509 are in use .

For any existing deployment prior to AEP 8.1.2 and where there is custom certificate configuration in place then a check is required before upgrade is implemented to determine if the x509 certificates in place are 2048-bit level.

If 1024-bit x509 certificates are in place, then they need to be removed and the appropriate level of x509 certificates need to be imported (2048-bit).

Failure to do this will result in features and services loss.

Note:

Where custom certificates have not been imported and the default certificates that come with AEP deployment are still in place are already created with 2048-bit x509 security certificates and no changes are required to upgrade to 8.1.2

5.3.2. Certificates in EPM Server

Experience Portal Manager (EPM) has two security certificates:

EP Signing Certificate (default install)

This security certificate is used to sign CSR's from Aux EPM , MPP and its own EPM certificate when in default configuration. This is called the EP Signing Certificate and is not used for any secure communication outside of signing CSR's.

This certificate must be removed when applying custom 3rd Party security certificates. Failure to remove this certificate will result in any Auxiliary EPM or MPP server custom certificates being replaced by this EP signing Certificate once they reboot

Note:

3rd Party custom security certificates and EP Signing certificate cannot be configured at some time. If the EP Signing certificate is put back on the solution when custom 3rd party certificates are installed, upon reboot of any of the servers, the EP Signing certificate will sign and overwrite those custom certificates with its own.

So, if the decision is to install 3rd party certificates, then one of the prerequisites is the removal of the EP Signing certificate on the Primary EPM.

Server Identity Certificate

The other is used for mutual authentication between the Primary EPM server and the Auxiliary EPM servers and the Media Processing servers and for mutual authentication with external servers such as the SIP Proxies and application servers.

5.3.3 Certificates in MPP and Auxiliary EPM

MPP and Auxiliary EPM both only have one security certificate each.

Server Identity Certificate

For mutual authentication between its server and the other EP servers and the Media Processing servers and for mutual authentication with external servers

such as the SIP Proxies and application servers

5.3.4 Server Identity Certificate Role

Server Identity Certificates are certificates that are used for establishing mutually authenticated secure communications between EPMs and MPPs. The **Server Identity Certificate** is also used for accessing the web pages and the web services.

During a fresh installation of Experience Portal servers, the installer generates self-signed certificates for the servers using the EP Signing Certificate which is also generated upon the installation process.

As part of a fresh installation, the installer also provides an option for importing a Server Certificate to be used in lieu of the default certificates if desired.

Experience Portal also provides a script to either import a new Server Identity Certificate for a server.

Details of the self-signed certificates generated by the installer during a fresh installation:

Version	Self-Signed Certificates
8.1 & above	SHA256 certificates with 2048 bit keys
8.0	SHA256 certificates with 2048 bit keys
7.0.1 & above	SHA256 certificates with 2048 bit keys
7.0	SHA128 certificates with 2048 bit keys
6.0.x	SHA128 certificates with 1024 bit keys

Support for using an externally generated chained certificate as the **Server Certificate** was added beginning with Experience Portal 7.0.1.

When importing an externally generated certificate to replace the server certificate, ensure the following:

- The certificate file is formatted as a PKCS#12 file. A PKCS#12 file always includes a certificate and the corresponding key. It is encrypted and requires a password.
- If the imported certificate is not a self-signed certificate, then the PKCS#12 file must include all the CA certificates in the signing chain.
- If the “Extended Key Usage” is specified in the X509.V3 certificate extension, specify “Server

Authentication” (also called “serverAuth”) and Client Authentication" (also called "clientAuth"), for the usage.

- Subject Alternative Name (SAN) – Must include SANs which are the Full qualified domain name of the server and the IP address of the server.

Import Server Certificate – Multiple Server Solution

Refer to the following topics in the “**Administering Avaya Aura Experience Portal – Security section**” document for detailed instructions on importing a new Server Certificate for a **multiple server** solution

- Importing a Primary EPM server security certificate
- Importing an Auxiliary EPM server security certificate
- Importing an MPP server security certificate

Import Server Certificate – Single Server Solution

Refer to the following topic in the “**Administering Avaya Aura Experience Portal Security Section**” document for detailed instructions on importing a new Server Certificate for a **single server** solution

- Importing a Single server security certificate

5.3.5 .EP Signing Certificate Role

Apart from the server Identity certificate, another certificate called the **EP Signing Certificate** is generated on the Primary EPM. This certificate is used for signing a certificate signing request (CSR) sent by the MPP and Auxiliary EPM. The MPP/Aux EPM uses the signed certificate to establish a mutually authenticated connection with servers that are configured to use the TLS transport. The administrator can replace the EP Signing certificate on the Certificates web page on the Primary EPM by either generating a new certificate from the Primary EPM Certificates web page or importing an externally generated certificate.

During a fresh installation of Primary EPM, Experience Portal generates self-signed certificates for the EP Signing Certificate.

Once the system is installed, it is possible to either import or generate a new EP Signing Certificate to be used in lieu of the root certificate that was generated during installation. A certificate signing request (CSR) can also be generated from the Certificates web page on the Primary EPM. This CSR can be signed by

an external certificate authority (CA) and then be imported as the EP Signing Certificate. Replacing of the EP Signing certificate can either be done using a command line script or through the EP Signing Certificate tab on the Certificates web page on the Primary EPM.

Details of the self-signed certificate generated by the installer during a fresh installation:

Version	Self-Signed Certificates
8.1 and above	SHA256 certificates with 2048 bit keys
8.0	SHA256 certificates with 2048 bit keys
7.0.1 & above	SHA256 certificates with 2048 bit keys
7.0	SHA128 certificates with 2048 bit keys
6.0.x	SHA128 certificates with 1024 bit keys

When importing an externally generated certificate to replace the EP Signing certificate, ensure the following:

- The certificate file is formatted as a PKCS#12 file. A PKCS#12 file always includes a certificate and its corresponding key. It is encrypted and requires a password.
- If the imported certificate is not a self-signed certificate, then the PKCS#12 file must include all the CA trusted certificates in the signing chain.
- If the “Extended Key Usage” is specified in the X509.V3 certificate extension, specify “Server Authentication” (also called “serverAuth”) and Client Authentication" (also called "clientAuth"), for the usage.
- The certificate must include the standard extension Basic Constraints with the **CA:true** attribute. [Note this is for the EP Signing Certificate only]

Generate/Import EP Signing Certificate

Refer to the following topic in the “**Administering Avaya Aura Experience Portal – Security section**” document for detailed instructions on generating or importing a new EP Signing Certificate from the EP Signing Certificate tab on the Certificates web page.

- Installing a EP Signing certificate for TLS authentication on EPM server

Import Third-Party Signed security certificate – Multiple Server Solution

Refer to the following topics in the "**Administering Avaya Aura Experience Portal – Security Section**" document for detailed instructions on importing a new third-party signed security certificate for a **multiple server** solution

- Importing a Primary EPM Third-Party signed security certificate
- Importing an Auxiliary EPM Third-Party signed security certificate
- Importing an MPP Third-Party signed security certificate

Import Third-Party Signed security certificate – Single Server Solution

Refer to the following topics in the "**Administering Avaya Aura Experience Portal Security Section**" document for detailed instructions on importing a new third party signed security certificate a **single server** solution

- Importing a Single server Third-Party Signed security certificate

5.3.6 Application Certificate Role

Third-Party security certificates can be installed on an application server to support certificate-based authentication for application reporting. Avaya Aura Orchestration Designer runtime interface supports uploading a third-party key store on an application server that can be used by a third-party speech application to perform authentication with the Application Logging web service on EPM. See Avaya Aura Orchestration Designer Developer's Guide for details.

5.3.7 Server Identity Validation

Starting with Experience Portal 7.2, the product includes support for performing server identity validation when establishing TLS communication with any server.

During a normal TLS handshake between the client and the server, the TLS client verifies the validity of the certificate, trusted CA and valid signature of the server certificate. Optionally the TLS client can perform an additional security check which is to authenticate the server's identity against the server certificate during the TLS handshake. The TLS client authenticates the server by verifying that the server is located at the network address specified by the domain name and/or IP address in the server certificate.

When Server Identity Validation is enabled, all the components of Experience Portal that act as a TLS client verify the identity of the remote server that it is establishing a connection with. TLS clients verify that the certificate asserts an identity in the certificate's Subject Common Name and/or Subject Alternate Name that matches the fully qualified domain name of the established connection. Once the validation succeeds, the secure communication is established otherwise the secure communication is not established with the server.

The following table lists the Experience Portal components that establish secure connections and perform additional security check if the Server Identity Validation is enabled:

Client	Server	Capability
Primary EPM	Auxiliary EPM	HTTPS Connections
Primary EPM	MPP	HTTPS Connections
MPP	Speech Server	MRCP V2 Connections
MPP	Session Manager	SIP TLS Connections
Primary EPM & Auxiliary EPM	SMS SMPP Gateway	SMPPS Connections
Primary EPM & Auxiliary EPM	SMS HTTP Server	HTTPS Connections
Primary EPM & Auxiliary EPM	Email Server	Email TLS Connections (SMTP, IMAP4 & POP3)
Primary EPM, Auxiliary EPM & MPP	Application Server	HTTPS Connections

Server identity validation can be enabled or disabled on the Security Settings web page under the Certificates web page. This capability is enabled by default for all fresh installs and disabled by default for system upgrades to prevent disruption of existing working systems.

Refer to **Server Identity Validation** topic in the "**Administering Avaya Aura Experience Portal**" document for best practices and basic trouble shooting tips for this feature.

6. Log Files and Audit Trails

Log files are useful for detecting suspicious system activity. Customers should implement a process to review log files on a regular basis.

6.1. Operating System Logging

The Linux operating system generates several logs that can be checked for evidence of possible security breaches. These logs include:

System	Filename	Contents
EPM/MPP	**/var/log/secure**	Console login access log
EPM/MPP	**/var/log/messages**	Various events, including use of the su command
MPP	**/var/log/httpd/access_log**	Apache HTTP Server log for HTTP connections
MPP	**/var/log/httpd/ssl_access_log**	Apache HTTP Server log for HTTPS connections

6.2.Experience Portal Audit Log

The Experience Portal system contains an Audit Log mechanism that collects important events for periodic review. All configuration changes made using the Web Administration utility are logged and include complete information on the values of changed fields. Companies can use the Experience Portal log to determine if any access or modifications to restricted resources or configuration setup have occurred. Similarly, this logging can be used to track addition or deletion of user IDs, password resets, and modifications of event logs and alarms. The Experience Portal system provides the date, time, user ID, and type of event for each event logged.

In addition to configuration changes, the audit log also tracks access to the Experience Portal system, recording logins and logouts of each user ID.

7.System Security

From Experience Portal 5.1 onwards, the EPM services (Avaya ActiveMQ, Avaya Service Locator and Apache Tomcat Server) run as a non-root user. The only service which runs as a root user is the SNMP Agent service as it needs to access ports which require root access.

Most of the services under services under MPP also run as a non-root user. The only service which runs as root user is the mppmon which needs to monitor the MPP services. Apart from this, there are two processes MediaManager and SessionManager which also run as root user as these processes need to escalate the threads to real time priority for performance and call handling.

Experience Portal installation modules create a non-root user called **avayavp** and a group called **avayavpgroup** on both the EPM and the MPP for this purpose. The installation modules also update the **/etc/security/limits.conf** file to ensure that different Experience Portal Linux users are configured with sufficiently high process limit and update the **/etc/sudoers** file to ensure that different Experience Portal Linux users have the required permissions for correct operation of Experience Portal.

8. Advanced Intrusion Detection Environment

Advanced Intrusion Detection Environment (AIDE) is a file integrity checker and intrusion detection program. AIDE can be run for checking the integrity of files to ensure the critical files have not been changed in an unauthorized manner. AIDE does this by creating a baseline database of files on an initial run, and then checks this database against the system on subsequent runs.

Experience Portal 7.2 onwards, the Red Hat AIDE package is installed under /user/sbin/aide folder. Only a Linux user with root privileges can run AIDE.

It is strongly recommended that the default AIDE configuration file (/etc/aide.conf) is reviewed and updated accordingly to match the customer server environment before running the AIDE tool.

Refer to Advanced Intrusion Detection Environment topic in the “Administering Avaya Aura Experience Portal” document for further details.

Refer to the Red Hat support site for detailed instructions on how to use the AIDE package.

9. System Access by Avaya Technicians

Customers who purchase service contracts will need to provide Avaya technicians with access to the Experience Portal system in the following circumstances:

- In response to an escalation
- In response to a service request
- The service request could be for regular maintenance or a software upgrade.
- When an alarm is reported by the Experience Portal system

All Experience Portal activities, whether they are generated by a service call or an alarm report, are tracked by the Avaya support organizations. Items that are tracked are:

- The technician who accessed the customer's machine
- When the access was made?
- What was done during the access, based on the ownership of the support case and the case notes entered by the support person?

Additionally, log files are maintained on the system that capture all commands entered, either locally or remotely.

An Experience Portal 7.2 system (Linux) that will be maintained by Avaya Technicians will need to be enabled for Enhanced Access Security Gateway (EASG) access.

EASG Enabled
EASG can be enabled either during installation of the system or later using the security tool (EASGConfigure.sh) installed as part of the system. When EASG is enabled, all the Avaya Service Accounts (**sroot**, **craft, inads** & **init**) are EASG protected by the challenge/response authentication. These logins are reserved for use by Avaya support personnel and should not be used for normal administration of the system.

EASG Disabled
When EASG is disabled, the **sroot**, **craft, inads** & **init** accounts are disabled and should remain as such. Assigning a password to one of the service accounts won't prevent its use for EASG access, but will weaken the security of that account, opening several vulnerabilities for exploitation.

In a bundled solution, two additional accounts (**cust** and **root**) are created with default passwords as **custpw** and **rootpw** respectively. The system will prompt for updating of the passwords for both these account on first root/sroot login.

Refer to the Enhanced Access Security Gateway topic "**Administering Avaya**

Aura Experience Portal" document for detailed instructions on enabling/disabling of EASG for the system. This topic also includes information about EASG utilities and EASG site certificate management.

10. Conclusion

No telecommunications system can be entirely free from the risk of unauthorized use. However, diligent attention to system management and to security can reduce that risk considerably. Often, a trade-off is required between reduced risk and ease of use and flexibility. Companies that use and administer their Experience Portal systems make this trade-off decision, know best how to tailor the system to meet their unique needs, and are in the best position to protect the system from unauthorized use. Because each company has ultimate control over the configuration and use of the Avaya services and products it purchases, the company properly bears responsibility for fraudulent uses of those services and products.