Proactive Outreach Manager

Security White Paper

Release 4.0
Issue 1.0
December 2020

Abstract

This paper provides information about the security strategy for Avaya Proactive Outreach Manager 4.0 and provides suggestions that companies can use to improve the security of their Proactive Outreach Manager systems and applications.

Contents

1. Overview

The Proactive Outreach Manager is a managed application residing on Experience Portal. Therefore, several system level security aspects of Experience Portal also apply to Proactive Outreach Manager. It is therefore advisable to refer to the Security White Paper published for Experience Portal in conjunction to the current document. Proactive Outreach Manager 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 Proactive Outreach Manager 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 Proactive Outreach Manager 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 Proactive Outreach Manager system.

3. Operating System Security

As noted earlier, Proactive Outreach Manager is a managed application residing on Experience Portal. Operating System level security aspects of Experience Portal also apply to Proactive Outreach Manager. It is therefore advisable to refer to the

Security White Paper published for Experience Portal in conjunction to the current document.

4. Network and Application Security

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 Proactive Outreach Manager deployed on Experience Portal installations, in which the Avaya Enterprise Linux Installer is used, only required network services will be installed and enabled.

For Proactive Outreach Manager deployed Experience Portal installations using Red Hat Enterprise Linux obtained from another vendor, ensure that only the required network services are installed and enabled.

More details on the network services, ports and connections needed by the Experience Portal can be found in the security document of the Experience Portal. Details of connections and ports used in Proactive Outreach Manager are mentioned inside the POM Port-matrix document.

Proactive Outreach Manager contains several services that communicate internally with each other, some services also communicate externally. These communications are described in the following sections.

3.1. External Communications

3.1.1. Agent Manager

The Agent Manager aka AM is one of POM's core components. It manages agent operations. The agent desktops built using Agent SDK communicate with the Agent Manager on TCP socket using port 9970 over TLS-1.2. The Agent Manager also interacts with different Avaya products such as Avaya Enablement Service on port 80/443, with Call Management System on port 7002, with Work Force Optimizer or Avaya Call Recorder on port 7998/7999, with Application Server on port 7778.

If external selection is enabled, then Agent Manager will communicate with the external selection system on port 11000.

3.1.2. Agent SDK Service

The Agent SDK Service serves as an interface between POM Widgets located in Workspaces for Elite (browser based Agent Desktop) and Agent Manager.

The Agent SDK Service communicates with POM Workspaces Elite on web-socket using port 6443 over TLS-1.2 by default. The port number and protocol can be configured from configuration file pomAgentSDKService.properties located on pom server at $POM_HOME/config. The default value of the environment variable $POM_HOME is /opt/Avaya/avpom/POManager.

Note here that the Agent Desktop applications built using Agent SDK communicate with the Agent Manager directly and not with the Agent SDK Service.

3.1.3. Kafka Server

Different POM processes internally publish events e.g. job events, agent events etc., on Kafka server and Kafka server sends these events to the clients that subscribe to it e.g. call recorder.

The Kafka server listens to incoming requests from the Event SDK clients on port 9093, the communication is over TLS-1.2.

3.1.4. vp_pom_service

The vp_pom_service is a web application that is deployed on the Apache Tomcat server. Proactive Outreach Manager leverages the Apache Tomcat server as provided by the Experience Portal. The vp_pom_service supports all REST APIs that are published by the Proactive Outreach Manager. Customers can get list and details of these REST APIs from the Proactive Outreach Manager's SDK document.

Proactive Outreach Manager also leverages the authentication and authorization as provided by the Experience Portal, which is required to communicate with the vp_pom_service. The communication is over https protocol on port 443.

3.2. Internal Communications

3.2.1. Campaign Manager

The Campaign Manager aka CM is one of POM's core components. It serves webservices requests from primary as well as auxiliary POM systems on port 9951. It interacts with Agent Manager on port 9995/10005, and with Rule Engine on port 8779.

3.2.2. Agent Manager

The Agent Manager aka AM is one of POM’s core components. It interacts internally with Campaign Manager on port 9995/10005, with another Agent Manager on port 8870, with Kafka server on port 9970, with Nailer/Driver applications on port 7778.

3.2.3. Campaign Director

The Campaign Manager aka CM is one of POM’s core components. It serves webservice requests from primary as well as auxiliary POM systems on port 9961.

3.2.4. Advanced List Management Service

Advanced List Management Service is a sprint boot service which handles file splitting activities. It communicates with VP_POM service and Campaign Director using REST APIs on port 8091 over TLS-1.2. The port number and protocol are not configurable.

3.2.5. Kafka Server

The Kafka server communicates with the co-resident zookeeper on open port 2181, which stores metadata. The access to this metadata can be restricted by enabling Zookeeper Authentication (Refer section ‘Enabling Zookeeper Authentication’ in ‘Implementing Avaya Proactive Outreach Manager’ document). If Kafka HA is also enabled, then ports 2888 and 3888 are also utilized.

3.2.6. Agent SDK Service

The Agent SDK Service serves as an interface between POM Workspace Elite (Agent Desktop built on Workspaces) and Agent Manager. It communicates internally with Agent Manager on TCP socket using port 9970 over TLS-1.2. The port number is configurable from the POM Home□ Global Configuration□ Agent manager base port.

3.2.7. Rule Engine

The Rule Engine evaluates rules for dialing as defined in the Rule Editor. On port 8779, it interacts with Campaign Manager, serves webservices requests as well as interacts with Rule Engine of other primary or auxiliary EPM.

3.2.8. ActiveMQ

The ActiveMQ is used for internal message exchange between several components internally. This message exchange is done on port 51616.

3.2.9. vp_pom

The vp_pom is a web application that is deployed on the Apache Tomcat server. Proactive Outreach Manager leverages the Apache Tomcat server as provided by the Experience Portal. The vp_pom application manages the Proactive Outreach Manager web user interfaces.

Proactive Outreach Manager also leverages the authentication and authorization as provided by the Experience Portal, which is required to communicate with the vp_pom. The communication is over https protocol on port 443.

3.2.10. POM Dashboard Service

The POM Dashboard Service monitors active campaigns and agents, and provides their status in real-time. The active campaign and agent data are read from kafka events. It listens for incoming requests on port 9097 and communicates over TLS-1.2.

3.2.11. POM Cache Service

The PomCacheService uses Apache Ignite and acts as in-Memory Database for operational data required for the dialing operations performed in POM. It communicates with other components of POM such as CM, CD & AM on port 6999. It also communicates with pom web module through socket connection on port 10800. The PomCacheService health-check is done on port 7445 over TLS-1.2.

4. TLS

POM is deployed as a managed application on Experience Portal. Web administration, user logins and passwords, are all maintained by Experience Portal. The Experience Portal Manager server aka EPM 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 Experience Portal Security white paper must be referred to get details on this.

Proactive Outreach Manager communicates over TLS-1.2 with external entities.

POM 4.0 supports FIPS 140-2. Ciphers used in TLS communications, Password encryption, Certificate management using Keystore and Truststore, as well as secure random number generation, are all done using FIPS compliant ciphers using the Cryptographic libraries provided by Bouncy Castle. By default, FIPS is disabled. Enabling FIPS is optional.

5. FIPS

5.1. AEP 7.2.3 FIPS Support

Provided OS-level compliance via script to install FIPS compliant RPM packages and modify Red Hat kernel configuration to ensure that only accredited cryptographic modules/ciphers are used.

5.2. AEP 8.0 FIPS enhancements - EPM

TLS connections and certificate access and management hardened to use Java objects from the Bouncy Castle FIPS Provider rather than the default non-FIPS compliant Sun security provider

Keystore and truststore managed by the EPM converted from Java default JKS format to FIPS compliant Bouncy Castle BCFKS format. A BCFKS keystore uses PBKDF2 with HMAC SHA512 for password to key conversion and AES CCM for encryption.

The BC FIPS provider also enforces FIPS compliant secure random number generation schemes

BC FIPS Java module awarded validation certificate #3585: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/3585

5.3. AEP 8.0 FIPS enhancements - MPP

Encryption of the RTP packet data for SRTP streams made FIPS-compliant by using OpenSSL rather than the rijndael-api-fst encryption library

OpenSSL FIPS Object Module 2.0 awarded validation certificate #1747: https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1747

6. Certificate Management

Self-signed certificates as well as certificates provided by a trusted certificate authority can be used with Proactive Outreach Manager. It is highly recommended to use industry compliant secured digital certificates with key length greater than equal to 2048 bits and signing algorithm as SHA2.

For details on using certificates with Proactive Outreach Manager, see the *Implementing Avaya Proactive Outreach Manager* guide.

7. Database

Proactive Outreach Manager currently supports MSSQL, Postgres, Oracle and MySQL databases. Communication between Proactive Outreach Manager and the Database can be chosen to be over secured channel. The database is owned by the customer, hence database hardening follows customer's requirements and their company policies. Proactive Outreach Manager uses the database intensively, to create schema and store configuration and other information in it, as well as for its normal operations. Customers must ensure to provide required database permissions, roles and users for Proactive Outreach Manager to use it. Kindly refer Proactive Outreach Manager product documentation for details on the database permissions, roles and users requirements.

8. Log Files and Audit Trails

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

Log files generated by various services of Proactive Outreach Manager are located at $POM_HOME/logs on the Proactive Outreach Manager server. The default value of the environment variable $POM_HOME is /opt/Avaya/avpom/POManager. Additionally, as the web applications get deployed on the tomcat server, their logs can be found at $CATALINA_HOME/logs. The default value of the environment variable $CATALINA_HOME/logs is /opt/Tomcat/tomcat.

The Experience Portal system contains an Audit log mechanism that collects important events for periodic review. Proactive Outreach Manager leverages the Audit log mechanism as provided by the Experience Portal. All configuration changes made using the Web Administration utility are logged and include complete information on the values of the changed fields.

9. System Access by Avaya Technicians

As POM is deployed as a managed application on Experience Portal, the access to the system is governed as per the details given by the Experience Portal product and security documentation, and the same should be referred when EASG is enabled or disabled.

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.